1xEV-DO Rel. 0, CELL SITE EMULATOR, & GEOLOCATION EXPERT REPORT

RE:

The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.)

By:

Daniel David Rigmaiden

May 29, 2013

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

Table of Contents

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

I, Daniel David Rigmaiden, declare[1] the following [May 29, 2013]:

I. Introduction

I am the defendant in United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz. "[A] party who is otherwise qualified as an expert may testify as an expert witness in his own case regardless of concerns that the party is plainly self-interested."[2] This declaration explains the independent operations of the FBI's cell site emulators, *etc.* used to intrude upon and locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden. The need for this declaration arises from the government's withholding of discoverable evidence relating to the cell site emulators used during the investigation leading to United States v. Rigmaiden. This declaration is separated into five sections: (1) Introduction, (2) Summary Of Conclusions, (2) Technical Explanations, (3) How The Aircard Was Intruded Upon, and (4) Daniel Rigmaiden's Expert Qualifications. Other than for Section V, the information provided in this declaration is taken from the *Technical Explanations* and *General Facts* section of my *Motion To Suppress* (Dkt. #824-1, Jun. 4, 2012), in United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz.

The noted information is now being provided in declaration form considering the district court in United States v. Rigmaiden refused to apply (1) the government's concession that "the

1. This declaration is being submitted under the protections of *Simmons*. *See* Simmons v. United States, 390 U.S. 377, 394 (1968) (Holding that "when a defendant testifies in support of a motion to suppress evidence on Fourth Amendment grounds, his testimony may not thereafter be admitted against him at trial on the issue of guilt unless he makes no objection."). I object to the government attempting to introduce this declaration as evidence at trial.

2. Masterson Marketting, Inc. v. KSL Recreation Corp., 495 F. Supp. 2d 1044, 1050 (S.D.Cal. 2007).

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

aircard tracking operation was a Fourth Amendment search and seizure[,]"[3] and (2) the government's concession and agreement to not contest my identification and classification of the various **independent** operations conducted by the StingRay and KingFish as being **separate** Fourth Amendment searches and/or seizures.[4] Rather than having applied the government's concessions when ruling on suppression issues,[5] the Court instead found that the FBI's use of the StingRay and KingFish to locate the aircard "was not a 'severe intrusion[,]'" *id.*, p. 13, and that the independent Fourth Amendment searches and seizures that I identified were merely "details of the device's operation [][and] clearly concern the manner in which the search was to be executed, something that need not be stated with particularity in the warrant." *Id.*, p. 27. In other words, the Court refused to apply the established "general assumption going into this motion... that intrusiveness is not an issue[]"[6] and that the government would not be permitted to make arguments to the likes of, "[w]ell, **that part** of what we did isn't a search because it's not intrusive."[7] Rather than find that each **part** was sufficiently intrusive to be a **separate** Fourth Amendment search and/or seizure—as was agreed on January 27, 2012—the Court instead found that my "efforts to parse the warrant requirement further are no more

3. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Government's Memorandum Re Motion For Discovery* (Dkt. #674, p. 1).

4. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, *January 27, 2012 Status Conference, Partial Transcript of Proceedings*, p. 13-23.

5. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Court's May 8, 2013 Order* (Dkt. #1009).

6. United States v. Rigmaiden, CR08-814-PHX-DGC, *January 27, 2012 Status Conference, Partial Transcript of Proceedings*, [THE COURT], p. 25.

7. *Id.* (emphasis added).

persuasive here than were the defendants' similar efforts in *Dalia* and *Brooks*."[8]

Because the Court ignored the established concessions and is effectively requiring me to meet a higher burden of proof, I am submitting this declaration for the record[9] in support of **(1)** *Motion To Suppress* (Dkt. #824-1), **(2)** *Motion For Reconsideration Of Portions Of Court's Order At Dkt. #1009 RE: Fourth Amendment Suppression Issues* (Dkt. #1033), **(3)** *Motion For Reconsideration Of Portions Of Court's Order At Dkt. #723 RE: Discovery Of StingRay And KingFish Evidence* (Dkt. #1037), and **(4)** *Motion Requesting Evidentiary Hearing To Settle Contested Issues Of Fact RE: Motions For Reconsideration Of Motion To Suppress And Motion For Discovery* (Dkt. #1038) in United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz.

II. Summary Of Conclusions

Based on Sections III and IV, *infra*, of this declaration, I was able to make the following summarized technical conclusions relating to the government intrusions upon the aircard, *etc.*:

1. The aircard (*i.e.*, the UTStarcom PC5740 Broadband Connection Card) is a High Rate Packet Data (HRPD) 1xEV-DO Rel. 0 Access Terminal with hybrid 1xRTT text message and 1xRTT low rate data service capabilities.

8. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Court's May 8, 2013 Order* (Dkt. #1009, p. 27).

9. The Court also denied my *Ex Parte Motion To Appoint 1xEV-DO Rel. 0, Etc. Expert To Defense* (Dkt. #866, CR08-814-PHX-DGC). *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Court's August 10, 2012 Order*, p. 1 (Dkt. #871) (denying motion for appointment of expert because, among other reasons, the proposed expert "has confirmed that Defendant's detailed technical arguments in the motion to suppress are correct[.]").

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

2. The aircard hardware is incapable of ringing or alerting to an incoming call and it does not allow for placing or receiving telephone calls (*i.e.*, wire communications). The aircard is not able to receive incoming voice calls or react to incoming voice pages under its factory configuration.

3. When accessing cell sites to receive wireless service, the aircard does not engage in "registration" as do cellular phones; instead, the aircard engages in "session establishment" and conducts "route updates,"

4. The aircard is a computer hardware "add-on card" that can only function when plugged into the PCMCIA slot of a host laptop computer.

5. In order to function, the aircard draws power from the host laptop computer, stores data on the hard drive of the host laptop computer, and its functions and operations are accessed through software installed on the host laptop computer.

6. The aircard was used to access the Verizon Wireless 1xEV-DO Rel. 0 data network and Verizon Wireless 1xRTT data network.

7. The aircard was not capable of generating real-time cell site location information when accessing the Verizon Wireless 1xEV-DO Rel. 0 and 1xRTT data networks.

8. Under its factory configuration, the aircard could not access the Verizon Wireless 1xRTT voice network.

9. Case agents identified the aircard hardware by tracing IP addresses that were temporarily assigned to the aircard by Verizon Wireless for the purpose of accessing the Internet through a Verizon Wireless aircard account.

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

10. Once identified, agents obtained 38 days of the aircard's historical cell site location information from Verizon Wireless and then used it to narrow the location of the aircard to an area covering *105,789,264 ft²*.

11. Using the historical cell site location information as the input data, the FBI employed triangulation techniques and location signature techniques to reduce the *105,789,264 ft²* location estimate by 93.9%, *i.e.*, to a *6,412,224 ft²* area.

12. After narrowing the historical aircard location to a *6,412,224 ft²* area, FBI technical agents had Verizon Wireless reprogram and write data to the aircard so that it would (1) recognize and connect to the FBI's cell site emulators, and (2) respond to the FBI's silent phone calls intended to force the aircard to drop its 1xEV-DO Rel. 0 data connection and generate real-time cell site sector location information via a 1xRTT voice connection.

13. After the reprogramming of the aircard, FBI technical agents made 32 silent phone calls (*i.e.*, pings) to the aircard over a six hour period. Considering the aircard is not a telephone and does not have telephone service or telephone hardware, the FBI's silent phone calls did not cause the aircard to "ring" and otherwise did not cause the aircard to notify the user that the FBI was calling the aircard.

14. Each of the FBI's 32 silent voice calls (over the noted six (6) hour period) forced the aircard to drop its 1xEV-DO Rel. 0 data connection (*i.e.*, a denial-of-service attack). After each silent voice call, the aircard was denied access to the Internet until a reconnection to the 1xEV-DO Rel. 0 data network could be attempted and established by the aircard user via the host laptop computer.

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

15. Each of the FBI's 32 silent voice calls also caused the aircard to generate and transmit real-time cell site sector location information to a 1xRTT Verizon Wireless cell site over a 1xRTT voice connection. Verizon Wireless then forwarded the real-time geolocation data to the FBI's SF-Martinez DCS-3000 Pen/Trap device via a connection from a Verizon Wireless network switch to the FBI DCS network.

16. Verizon Wireless buffered the aircard's real-time cell site sector location information prior to transmission but did not first record and store the data prior to forwarding it to the FBI, *i.e.*, there was no transmission "after receipt and storage."

17. FBI technical agents used the aircard's real-time cell site sector location information to narrow the geographical area of where to precisely search for the aircard. In order to pinpoint the exact location of the aircard, FBI technical agents used the Harris brand StingRay (vehicle-transportable cell site emulator), Harris brand KingFish (hand-held man-portable cell site emulator), Harris brand AmberJack (phased array beam-forming antenna), and related cell site emulator equipment.

18. After each silent voice call placed to the aircard, FBI technical agents operated the vehicle-transportable StingRay with AmberJack antenna in the geographical area identified by the aircard's real-time cell site sector location information. Using the StingRay, FBI technical agents broadcast an emulated 1xEV-DO Rel. 0 data network signal in hopes that the aircard would detect the network as preferable and conduct an Idle State Route Update (*i.e.*, handoff) to the StingRay during one of the reconnect attempts following each dropped Verizon Wireless 1xEV-DO Rel. 0 data connection caused by the FBI's silent phone calls.

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

19. After the 32nd silent voice call, the aircard's attempt to reestablish the dropped Verizon Wireless 1xEV-DO Rel. 0 data connection resulted in the aircard establishing a 1xEV-DO Rel. 0 data connection with the FBI's StingRay. The StingRay was able to hijack the aircard's signal from Verizon Wireless and secretly send/receive signals to/from the aircard while portraying itself as a Verizon Wireless cell site.

20. FBI technical agents had the StingRay write data to the aircard's internal storage device. The data written to the aircard corresponded directly to the StingRay and would not have been written to the aircard by the Verizon Wireless network.

21. FBI technical agents had the StingRay deactivate 1xEV-DO Rel. 0 security layer encryption while communicating with the aircard. Because the FBI failed to implement standard security layer encryption over the air interface, the aircard's signals containing private information (*e.g.*, the ESN via the HardwareIDRequest message, geolocation data, *etc.*) were exposed to third-parties over the air interface.

22. FBI technical agents used the StingRay to download data stored on the aircard's internal storage device (*i.e.*, the aircard's Electronic Serial Number (ESN)).

23. FBI technical agents used the StingRay to send location finding interrogation signals through the walls of private areas and into the aircard in order to search out the location of the aircard and its user. The StingRay transmitted specially crafted location finding interrogation signals to the aircard. In response to the location finding interrogation signals, the aircard responded by sending location finding response signals which were used by the StingRay for geolocation calculations.

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

24. While using the StingRay during interrogation, FBI technical agents used the AmberJack phased array beam-forming antenna to transmit a highly directional and concentrated beam of location finding interrogation signals into apartment No. 1122 and other private areas. The AmberJack antenna is different from cell site antennas in the effect that it is capable of facilitating highly precise angle-of-arrival measurements in order to obtain a line-bearing to a target wireless device.

25. FBI technical agents collected the aircard's signal transmissions sent in response to the location finding interrogation signals sent to the aircard by the FBI via the StingRay. The signals in question were generated and transmitted by the aircard upon the StingRay's specific instruction (via the location finding interrogation signals) and would not have been transmitted during the aircard's communications with actual Verizon Wireless cell sites.

26. In order to determine the location of the aircard and its user, FBI technical agents conducted triangulation techniques on the aircard's location finding response signals collected by the StingRay. FBI technical agents engaged in active approach to facilitate triangulation of the collected location finding response signals transmitted by the aircard. The active approach method involves using the StingRay in cell site emulator mode to collect and measure location finding response signals at one location and then repeatedly moving the StingRay to new locations for additional collection and measurement.

27. FBI technical agents conducted numerous geolocation measurements on collected aircard signals. The geolocation measurement techniques included time-of-flight, power-distance, angle-of-arrival, statistical functions, and data fusion. The geolocation measurement

techniques used by FBI technical agents meet the definition of triangulation in the geolocation context.

28. Shortly before 4:45pm on July 16, 2008, FBI technical agents were able to triangulate the location of the aircard and its user as being somewhere within the Domicilio apartment complex in Santa Clara, CA.

29. Once the location of the aircard and its user was narrowed to a geographical area including the Domicilio apartment complex, FBI technical agents stopped using the StingRay and began using the second cell site emulator, *i.e.*, the hand-held man-portable KingFish.

30. Because geolocation evidence was destroyed by the FBI, the precise geographical and temporal point at which FBI technical agents stopped using the StingRay and started using the KingFish in unknown. It is known, however, that the StingRay first narrowed the location of the aircard to a geographical area which included the Domicilio apartment complex. This area may have been larger or smaller than the entirety of the Domicilio property.

31. The KingFish operates nearly identical to the StingRay with the only relevant difference being that it is a man-portable wireless device locator, as apposed to a vehicle-transportable wireless device locator, and is capable of locating wireless devices more accurately than the StingRay. Therefore, all of the independent operations conducted during use of the StingRay were repeated by FBI technical agents during use of the KingFish.

32. The KingFish was used by FBI technical agents on foot within the the Domicilio property. Using the KingFish, FBI technical agents were able to pinpoint the precise location of the aircard and its user as being within apartment No. 1122 of the Domicilio apartment

complex.

33. Whenever the aircard was connected to either the StingRay or KingFish, FBI technical agents denied the aircard access to the Internet (*i.e.*, a denial-of-service attack). Because the StingRay and KingFish are not capable of forwarding communications content to Verizon Wireless, the aircard user was not provided with any Internet access service. Using the StingRay and KingFish, FBI technical agents conducted a denial-of-service attack on the aircard for nearly 10 hours.

34. The StingRay and KingFish relied upon the electricity provided to the aircard by its user. Because FBI technical agents were forcing the aircard to generate and transmit radio waves that were subsequently collected and decoded by their surveillance equipment, the FBI was relying upon (*i.e.*, using) the electricity being provided to the aircard.

35. FBI technical agents had the StingRay and KingFish send the aircard commands instructing it to increase its signal transmission power to facilitate more effective geolocation. In order to more precisely search for and locate the aircard while using the StingRay and KingFish, FBI technical agents sent RPC bits to the aircard causing it to transmit at a higher power. This increase in transmission power increased the amount of electricity hijacked from the host laptop computer and ultimately from apartment No. 1122.

36. Approximately 18 days after the aircard was located, *i.e.*, shortly after my arrest, FBI technical agents destroyed all of the real-time geolocation data and other data collected by the StingRay and KingFish.

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

III. Technical Explanations

The proceeding subsections provide detailed technical information on communications protocols, geolocation techniques, surveillance equipment, surveillance programs, and investigative methods used by the government to intrude upon and locate wireless devices.[10] This background information is required in order to sufficiently understand how the UTStarcom PC5740 aircard was, searched, seized, and located in the investigation leading to United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz.

A. Electromagnetic radiation in the radio frequency band.

Radio waves are one type of electromagnetic radiation within the electromagnetic spectrum. "The electromagnetic spectrum contains radio waves, microwaves, light, x-rays, and gamma rays."[11] "Every wave has three different properties: (1) wavelength (a spatial measurement), (2) frequency (a temporal measurement), and (3) energy (or equivalently mass)."[12] "We can always find the frequency of a wave if we know its wavelength. Or, if we know the frequency, we can find its wavelength. The reason is that the frequency multiplied by the wavelength of a wave must always give a product equal to the velocity of light. This is true

10. The facts contained in this section are meant to reflect a "snapshot" of how the technology existed as of July of 2008—even while some newer technical sources are cited.

11. The Southwestern Company, *The Volume Library: A Modern, Authoritative Reference for Home and School Use*, "Wave theory" (Nashville, TN: The Southwestern Company, 1989), p. 460 (diagram labeled "Electromagnetic Spectrum").

12. Boatmun, Dewey L., *Quantum World: The Wave Nature of Our Universe* (Xlibris Corporation, 2010), p. 63.

of all electromagnetic waves."[13] In radio communications, electromagnetic waves are classified in terms of frequency.[14] For example, the specific radio frequencies licensed to Verizon Wireless for its cdma2000 based cellular network (*e.g.*, 1xRTT, 1xEV-DO, *etc.*) in the San Jose, CA market area are (1) 835 - 845 MHz paired with 880 - 890 MHz and 846.5 - 849 MHz paired with 891.5 - 894 MHz;[15] and (2) 1850 - 1865 MHz and 1930 - 1945 MHz.[16][17]

13. Lapp, Ralph E., "Radiation," *The World Book Encyclopedia*, Q-R, Volume 15 (Chicago, IL: Field Enterprises Educational Corporation, 1962), p. 76.

14. For a "spectrum activity"chart showing *some* electromagnetic frequencies used by modern day radio communication systems, *see* Thales [PDF presentation], "New solutions for massive monitoring", *ISS World Europe*, p. 4 (Oct. 3, 2008), *available at* http://wikileaks.org/spyfiles/files/0/40_200810-ISS-PRG-THALES.pdf (last accessed: Apr. 10, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 058 of *2nd Consolidated Exhibits* (Dkt. #821-3) ("spectrum activity" chart attached).

15. *See* FCC [website], *ULS License - Cellular License - KNKA211 - GTE MOBILNET OF CALIFORNIA LIMITED PARTNERSHIP*, http://wireless2.fcc.gov/UlsApp/UlsSearch/license.jsp?licKey=12154 (last accessed: Mar. 4, 2012); FCC [website], *ULS License - Cellular License - KNKA211 - GTE MOBILNET OF CALIFORNIA LIMITED PARTNERSHIP – Frequencies*, http://wireless2.fcc.gov/UlsApp/UlsSearch/frequenciesCell.jsp?licKey=12154&channelBlock=B (last accessed: Mar. 4, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 059 of *2nd Consolidated Exhibits* (Dkt. #821-3) (license documents attached).

16. *See* FCC [website], *ULS License - PCS Broadband License - WQIQ264 - Verizon Wireless Telecom Inc.*, http://wireless2.fcc.gov/UlsApp/UlsSearch/license.jsp?licKey=3003123 (last accessed: Apr. 9, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 060 of *2nd Consolidated Exhibits* (Dkt. #821-3) (license document attached).

17. Although Verizon Wireless' license data indicates a small number of listed cell site locations, "[a] licensee may operate additional transmitters at additional locations on the same channel or channel block as its existing system without obtaining prior Commission approval provided: [] (1) The interfering contours of the additional transmitter(s) must be totally encompassed by the composite interfering contour of the existing station (or stations under common control of the applicant) on the same channel..." 47 CFR § 22.165 *et seq*.

[18] Radio waves, as well as all other electromagnetic radiation, "propagate at the speed of light: 186,282 miles per second."[19] Radio wave propagation can be in the form of either omnidirectional radio waves or directional radio waves. "Omnidirectional ('all directions') radio-frequency propagation can be compared to the waves created by throwing a pebble into a pond. The waves made by the pebble emanate in all directions equally."[20] Directional radio frequency propagation by contrast have more gain (*i.e.*, signal coverage area) in certain directions and less in others.[21] Directional radio frequency propagation can therefore be thought of as a "ray" or "beam" of radio waves directed at a certain area.

In addition to wave like properties, radio waves also have particle like properties.[22]

18. Although Verizon Wireless' cdma2000 based mobile network operates on both the "Cellular" spectrum (KNKA211) and "PCS" spectrum (WQIQ264), the network itself remains constant with the only difference being the range of frequencies used over the air interface. For simplicity purposes, Verizon Wireless' cdma2000 based mobile network will be referred to as a cellular network regardless of any possible spectrum in use.

19. Bedell, Paul, *Cellular/PCS Management: A Real World Perspective*, (New York, NY: McGraw-Hill Professional Publishing, Mar. 31, 1999), p. 38.

20. *See id*.

21. *See* United States Army, *Communications-Electronics Fundamentals: Wave Propagation, Transmission Lines, and Antennas,* Training Circular 9-64 (Washington, DC: July 2004), *available at* http://www.cbtricks.com/miscellaneous/tech_publications/neets/tc9_64.pdf (last accessed: April 10, 2012), p. 4.11 (PDF, p. 177) ("Some antennas are highly directional; that is, more energy is propagated in certain directions than in others. The ratio between the amount of energy propagated in these directions compared to the energy that would be propagated if the antenna were not directional is known as its gain. When a transmitting antenna with a certain gain is used as a receiving antenna, it will also have the same gain for receiving. ").

22. Lapp, "Radiation," *The World Book Encyclopedia*, Q-R, Volume 15, p. 78 ("We no longer worry about trying to pin down a radiation and ask whether it is a wave or a particle. We know that it may behave as both."); *see also* Levi, A. F. J., *Applied Quantum Mechanics*, 2nd ed. (Cambridge, NY: Cambridge University Press, 2006), p. 76 ("Using what we know from

"Light rays, heat radiation, radio waves, X rays, cosmic rays, and gamma rays produced by splitting atoms are all streams of photons."[23] Electromagnetic radiation can therefore be visualized as a stream of photons[24] traveling at the speed of light. A photon is an atomic particle[25] produced when an electron changes from a high energy level to a low energy level.[26] Although a photon cannot be weighed, streams of photons still exhibit an observable mass. "For one thing, light produces a definite pressure when it falls on an object. As a comet moves around the sun, its great gaseous tail is always streaming out away from the sun. This can be satisfactorily explained only by assuming that the light from the sun pushes the tail away."[27] Photons also carry energy which is directly proportional to frequency.[28] This photon energy can be converted into electricity for practical applications. For example, when transmitted

classical mechanics and electrodynamics and considering the ramifications of the Young's slits experiment and the photoelectric effect forced us to create the concept of particles with wavy character.").

23. Lapp, "Radiation," *The World Book Encyclopedia*, Q-R, Volume 15, p. 74.

24. *Id.* ("Radiation is the term used to describe any stream of photons.").

25. Lapp, Ralph E. (critically reviewed by Glenn T. Seaborg), "Atom," *The World Book Encyclopedia*, A, Volume 1 (Chicago, IL: Field Enterprises Educational Corporation, 1962), p. 705 (table of "Known Atomic Particles" with photon listed).

26. *See id.*, p. 706 ("This energy-level theory serves to explain how atoms can give off radiant energy, such as light. The amount of energy given off by an electron in changing to a lower energy level produces a *photon*, or unit, of a certain energy." (internal citation omitted)).

27. Lapp, "Radiation," *The World Book Encyclopedia*, Q-R, Volume 15, p. 78.

28. "[T]he larger the frequency of the light beam, the more energy in each photon of light." Bewick, Sharon, *et al.*, CK-12 Foundation, *CK-12 Chemistry* (FlexBook, Feb. 15, 2012), *available at* http://www.ck12.org/flexbook/pdf/6d8f3b870516db645033c94b3bf9fe31.pdf (last accessed: May 6, 2012), p. 161. "The full spectrum of electromagnetic radiation has radio waves as its lowest energy, lowest frequency, longest wavelength end and gamma rays as its highest energy, highest frequency, shortest wavelength end." *Id.*, p. 152.

radio waves reach a receive antenna,[29] the photon energy induces a voltage in the antenna producing a current of electricity which transfers the radio signals from the antenna to the receiver.[30] The photon energy produced by radio waves is small when compared to other electromagnetic radiation but it is still strong enough to power, for example, an AM radio receiver and speaker—without a separate power source—if close enough to an AM transmitter.[31]

B. The 1xEV-DO cellular communications system deployed by Verizon Wireless.

1. Origins of the 1xEV-DO cellular communications system.

The 1xEV-DO cellular communications system is defined within the cdma2000 family of standards developed by the 3rd Generation Partnership Project II (3GPP2).[32] These

29. "An antenna is a conductor or a set of conductors used either to radiate electromagnetic energy into space or to collect this energy from space." United States Army, *Communications-Electronics Fundamentals: Wave Propagation, Transmission Lines, and Antennas*, p. 1.34 (PDF, p. 46). "After an RF signal has been generated in a transmitter, some means must be used to radiate this signal through space to a receiver. The device that does this job is the antenna. The transmitter signal energy is sent into space by a transmitting antenna; the RF signal is then picked up from space by a receiving antenna." *Id.*, p. 4.4 (PDF, p. 170).

30. "The RF energy is transmitted into space in the form of an electromagnetic field. As the traveling electromagnetic field arrives at the receiving antenna, a voltage is induced into the antenna (a conductor). The RF voltages induced into the receiving antenna are then passed into the receiver and converted back into the transmitted RF information." *Id*.

31. Hayes, Arthur H., "Radio," *The World Book Encyclopedia*, Q-R, Volume 15 (Chicago, IL: Field Enterprises Educational Corporation, 1962), p. 88, Diagram labeled "A Simple Radio Set" ("A Crystal Set is a simple radio that does not use electricity."); Tymony, Cy, *Sneaky Uses for Everyday Things* (Kansas City, MO: Andrews McMeel Publishing, 2003), p. 60 ("Even now, many parents show their kids how to make a radio at home that doesn't require AC power or batteries.").

32. *See* Etemad, Kamran, *cdma2000 Evolution: System Concepts and Design Principles*

standards define a set of specifications that cellular device manufacturers and cellular service providers must follow to ensure compatibility across hardware and networks.[33] The cdma2000 family of standards, including 1xEV-DO, is based on a communications protocol[34] called code division multiple access (CDMA) originally designed for military use[35] due to it being nearly impossible to intercept a CDMA signal.[36] In the United States, there are various CDMA cellular service providers including "Alaska Communications System, Carolina West, CellCom/nSight, Bluegrass Cellular, Leap Wireless, Sprint, U.S. Cellular, and Verizon Wireless."[37]

"CDMA employs what is known as wideband *spread spectrum* technology to carry

(Hoboken, NJ: John Wiley & Sons, Inc., 2004), p. xiii, 4 and 9. *See also* http://www.3gpp2.org.

33. *See* Telecommunications Industry Association, TIA-2000.1-E, *Introduction to cdma2000 Spread Spectrum Systems* (Arlington, VA: Oct. 2009), § 1.1.1, p. 1.1.

34. "Protocol: A standard set of definitions governing how communications are formatted in order to permit their transmission across networks and between devices." CTIA [website], *Wireless Glossary of Terms N-P*, http://www.ctia.org/media/industry_info/index.cfm/AID/10407 (last accessed: Aug., 30, 2011).

35. *See* Levine, R.C., *Digital Switching: Cellular & PCS Lectures April 17 & 24, 2001*, Beta Scientific Laboratory, Inc., (Richardson, TX: 1996-2000), *available at* http://www.privateline.com/levine/CELPCS4.PDF (last accessed: Sept. 29, 2010), p. 59 ("CDMA was first developed for military point-to-point communications.").

36. *See* Bedell, *Cellular/PCS Management: A Real World Perspective*, p. 225 ("CDMA was originally deployed as a battlefield communications system because it is very hard if not completely impossible to intercept CDMA transmissions.").

37. CTIA [website], Glossary of Terms C-D, http://www.ctia.org/media/industry_info/index.cfm/AID/10321 (last accessed: Aug., 30, 2011) (defining CDMA).

digitized voice and data transmissions."[38][39] Spread spectrum technology spreads "the radio signal over a wide frequency range by modulating it with a code word unique to the radio."[40] The receiver "distinguishes [the] sender's signal from other signals by examining the wide spectrum band with a time synchronized duplicate of the spreading code word."[41] In simple terms, CDMA in cellular telephony is "[a] technology used to transmit wireless calls by assigning them codes[]"[42] allowing for each CDMA transmitter to transmit simultaneously to a single cell site without having the signals conflict with each other.[43] On the reverse link, "[t]his process is analogous to each mobile speaking a different language and the base station

38. Bedell, *Cellular/PCS Management: A Real World Perspective*, p. 226.

39. Issued in 1942, "[t]he U.S. patent for spread-spectrum technology was held jointly by actress Hedy Lamarr and music composer George Antheil." Muller, Nathan J., *Bluetooth Demystified* (New York, NY: McGraw-Hill, Sept. 8, 2000), p. 61 (figure note omitted). "Spread spectrum has two modes of operation: frequency hoping and direct sequencing. *Frequency hoping* spreads its signals by 'hoping' the narrowband signal over the entire radio band as a function of time. *Direct sequencing* spreads its signal by expanding the signal all at once over the entire radio band." *Id.*, p. 63. CDMA uses direct sequencing.

40. Katz, Randy H., Professor at U.C. Berkeley, CS 294-7: Media Access—TDMA and CDMA, p. 13 (1996), *available at* http://www.sss-mag.com/pdf/1tdmacdma.pdf (last accessed: Aug. 31, 2010); *see also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 11 ("The basic idea of spread spectrum communications is based on transmitting information over channels much wider than required by the original signal bandwidth. The spread spectrum term is used to reflect the fact that the system spreads the energy of the information signal over a much wider band channel, allowing signal transmission at very low power spectral densities.").

41. *Id*.

42. CTIA [website], Glossary of Terms C-D, http://www.ctia.org/media/industry_info/index.cfm/AID/10321 (last accessed: Aug., 30, 2011) (defining CDMA).

43. Katz, CS 294-7: Media Access—TDMA and CDMA, p. 19.

interpreting each of the languages it receives."[44] In all CDMA based cellular systems, the term "reverse link" refers to the signal path leading from the wireless device to the cell site and the term "forward link" refers to the signal path leading from the cell site to the wireless device.[45]

CDMA was first introduced in cellular systems in the early 1990s with the cdmaONE family of standards.[46] Cellular communications systems based on cdmaONE began with "voice only" services (*see* IS-95A) with limited data services added later (*see* IS-95B).[47] After commercial use of cdmaONE throughout the 1990s, the cellular communications industry developed cdma2000 beginning with the IS-2000 Release 0 technical standard, which is also referred to as 1xRTT.[48] 1xRTT, first commercially deployed in the year 2000,[49] provides both voice and data services[50] with performance increases over cdmaONE technology. Later that year, 3GPP2 set out to improve upon 1xRTT by drafting and publishing the cdma2000 High-Rate Packet Data (HRPD) standard referred to as IS-856 or 1xEV-DO (an acronym for

44. Bedell, *Cellular/PCS Management: A Real World Perspective*, p. 226.

45. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 31, Fig. 3.4.

46. *See id.*, p. 6.

47. *See id.*, p. 6-7.

48. *See id.*, p. 7-8.

49. *See id.*, p. 8.

50. *See* eogogicsinc (website), *cdma2000 Technologies: 1xRTT, EVDO, UMB, and EVDV*, "cdma2000 Technology Family: 1xRTT, EVDO, UMB, and EVDV: What Is cdma2000?," http://www.eogogics.com/talkgogics/tutorials/cdma2000 (last accessed: Jun. 9, 2011) (showing a diagram with 1xRTT supporting "High Capacity Voice" and "Packet Data").

EVolution Data-Optimized).[51][52] The original release of 1xEV-DO, first commercially deployed in the year 2002,[53] is referred to as "Release 0" (or "Rel. 0") and subsequent releases are referred to as "Revision A," "Revision B," and "Revision C" with each revision adding features and increasing data rates[54] All versions of 1xEV-DO use cellular networks to provide broadband Internet access to Access Terminals such as aircards. Unlike 1xRTT, 1xEV-DO does not allow for placing voice calls and is strictly limited to data services.[55]

The remainder of the technical explanations contained in this section are presented in the context of 1xEV-DO Rel. 0—the version of 1xEV-DO used by the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.). All cell sites, including FBI cell site emulators, that wish to send or receive radio signals to/from a 1xEV-DO Rel. 0 based Access Terminal **must** follow the detailed instructions outlined in the cdma2000 technical standards applicable to 1xEV-DO Rel. 0. "The technical requirements contained in cdma2000 form a compatibility standard for CDMA systems. They ensure that a mobile station

51. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 9.

52. *See* Qualcomm Inc., EV-DO Rev. A and B: Wireless Broadband for the Masses (whitepaper), *The History of Mobile Broadband*, p. 3 ("With EV-DO, consumers experienced 400-600 Kbps of average downlink throughput with bursts up to 2.4 Mbps - 4 to 10 times faster than data over CDMA2000 1X (also referred to as 1xRTT) or UMTS networks.").

53. *See id*.

54. *See* eogogicsinc (website), *cdma2000 Technologies: 1xRTT, EVDO, UMB, and EVDV.*

55. *See* Chuah, Mooi Choo and Zhang, Qinqing, *Design And Performance Of 3G Wireless Networks And Wireless LANs* (New York, NY: Springer Science+Business Media, Inc., 2006), p. 66 ("The network architecture of 1xEV-DO is very similar to the 3G1x network architecture except that the components associated with voice traffic are absent.").

can obtain service in a system manufactured in accordance with the cdma2000 standards."[56] The primary technical standards relevant to 1xEV-DO Rel. 0 are listed below:

1. Telecommunications Industry Association, TIA/EIA/IS-856-1 (Addendum No. 1 to TIA/EIA/IS-856), *cdma2000 High Rate Packet Data Air Interface Specification* (Arlington, VA: Jan. 2002); **Note:** IS-856-1 sets forth standards dictating the technical requirements for HRPD "Release 0" (*i.e.*, 1xEV-DO Rel. 0) systems and is primarily oriented toward requirements necessary for the design and implementation of Access Terminals. The original cdma2000 HRPD technical standard is IS-856, released by 3GPP2 in November of 2000.[57] However, in January of 2002, 3GPP2 released IS-856-1[58] and in March of 2004, IS-856-2[E] [59]—all of which expanded upon the original IS-856 specification as applicable to 1xEV-DO Rel. 0.[60] For the technical explanations outlined in this section, IS-856-1 is referenced.

2. Telecommunications Industry Association, ANSI/TIA-878-2 (Addenda to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network* (Arlington, VA: May 2008); **Note:** IS-878-2 sets forth standards dictating Access Terminal authentication, handoffs, Hybrid

56. *See* TIA-2000.1-E, *Introduction to cdma2000 Spread Spectrum Systems*, § 1.1.1, p. 1.1.

57. *See* Telecommunications Industry Association, TIA/EIA/IS-856, *cdma2000 High Rate Packet Data Air Interface Specification* (Arlington, VA: Nov. 2002).

58. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*.

59. *See* Telecommunications Industry Association, TIA-856-2[E], *cdma2000 High Rate Packet Data Air Interface Specification – Addendum 2* (Arlington, VA: Mar. 2004).

60. The differences between the three noted cdma2000 HRPD "Release 0" standards are negligible in the context of the aircard locating mission in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.).

Access Terminal (HAT) operations, *etc.* in an HRPD system. The original cdma2000 HRPD Interoperability standard is IS-878, released by 3GPP2 in December of 2001.[61] However, in May of 2003, 3GPP2 released IS-878-1[62] and IS-1878,[63] and in May of 2008, IS-878-2[64] and IS-1878-1[65]—all of which expanded upon the original IS-878 specification as applicable to 1xEV-DO.[66] For the technical explanations outlined in this section, IS-878-2 is referenced.

3. Telecommunications Industry Association, TIA-683-D (Revision to TIA-683-C), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, (Arlington, VA: May 2006); **Note:** IS-683-D sets forth standards dictating the Over-the-Air Service

61. *See* Telecommunications Industry Association, ANSI/TIA-878, *Inter-Operability Specification (IOS) for High Rate Packet Data (HRPD) Network Access Interfaces* (Arlington, VA: Dec. 2001); Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 265 ("The enhanced 1X-EV DO network supports enhancements in IOS interface, captured in IS878, allowing access authentication and interface between two access networks.").

62. *See* Telecommunications Industry Association, ANSI/TIA-878-1 (Addendum No. 1 to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces – Addendum 1* (Arlington, VA: May 2003).

63. *See* Telecommunications Industry Association, ANSI/TIA-1878, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces – Alternative Architecture* (Arlington, VA: May 2003).

64. *See* Telecommunications Industry Association, ANSI/TIA-878-2 (Addenda to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network* (Arlington, VA: May 2008).

65. *See* Telecommunications Industry Association, ANSI/TIA-1878-1 (Addendum to TIA-1878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Packet Control Function* (Arlington, VA: May 2008).

66. Considering the differences between these standards are negligible in the context of the aircard locating mission in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.), IS-878-2 (May 2008) will be used as the primary technical reference in this section.

Provisioning (OTASP) of Mobile Station and HRPD (*i.e.*, 1xEV-DO) Access Terminal operational parameters. The original Over-the-Air Service Provisioning standard is IS-683, which was subsequently updated by 3GPP2 via IS-683-A in June of 1998.[67] However, in December of 2001, 3GPP2 released IS-683-B,[68] in March of 2003, IS-683-C,[69] and in May of 2006, IS-683-D.[70] For the technical explanations outlined in this section, IS-683-D is referenced.

The remainder of this section will cite to the above 3GPP2 technical standards and to other relevant technical references. Some technical references will be specific to older cellular technology (*e.g.*, 1xRTT or IS-95A/B) but are only cited to the effect they provide information that remains constant through later CDMA technology, *i.e.*, 1xEV-DO Rel. 0.[71][72] In those

67. *See* Telecommunications Industry Association, TIA-683-A (Revision of TIA/EIA/IS-683), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, (Arlington, VA: Jun. 1998).

68. *See* Telecommunications Industry Association, TIA-683-B (Revision of TIA/EIA-683-A), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems* (Arlington, VA: Dec. 2001).

69. *See* Telecommunications Industry Association, TIA-683-C (Revision of TIA/EIA-683-B), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems* (Arlington, VA: Mar. 2003).

70. *See* TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

71. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, Forward, p. xlix ("This standard is evolved from and is a companion to the cdma2000 standards."); Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 264 ("The network architecture in HRPD is similar to the IS2000 system with some variations in network elements, functionalities, and interface protocols.").

72. Proceed with caution if references addressing older CDMA technology are pulled and studied for further information. 1xEV-DO, being a pure data network, does not adopt the

cases, the term "Mobile Station" should be read as "Access Terminal," and the term "Base Station" should be read as "Access Network."

2. Basic hardware elements of a 1xEV-DO Rel. 0 compatible cellular data network.

a. The Access Terminal (AT).

The basic hardware elements of a 1xEV-DO Rel. 0 cellular data network have both similarities and differences when compared to a 1xRTT cellular voice network. A 1xEV-DO Rel. 0 data network begins with the Access Terminal (AT), which consists of a radio transmitter/receiver (transceiver), antenna, and other hardware used for communicating with Access Networks.[73] The Access Terminal is the equivalent of a Mobile Station (MS) (*i.e.*, cellular telephone) in 1xRTT.[74] The Access Terminal "may be a self-contained data device such as a personal digital assistant (PDA) or a detachable module that is connected to a computing device such as a laptop personal computer."[75] From a legal perspective, the difference between an Access Terminal and a Mobile Station is that the former facilitates the sending/receiving of electronic communications[76] while the later facilitates the

majority of the subject matter specific to IS-95A/B, 1xRTT, *etc*.

73. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (example of an Access Terminal).

74. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 264.

75. *Id*.

76. *See* 18 U.S.C. § 2510(12) ("'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce, but does not include--(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a

sending/receiving of wire communications.[77] However, most 1xEV-DO Rel. 0 based wireless devices are "Hybrid mobile stations / Access Terminals (HATs),"[78] *i.e.*, they support both 1xRTT wire communications and 1xEV-DO Rel. 0 electronic communications.[79] "Hybrid mode device[s]... support cdma20001x and HRPD by periodic[ly] monitoring the paging channel of cdma20001x[] [(*i.e.*, 1xRTT)]"[80] but cannot maintain 1xEV-DO and 1xRTT traffic channels simultaneously. If a Hybrid Access Terminal lacks the hardware required to place voice calls,[81] such as a PCMCIA broadband Internet access card (*i.e.*, aircard), the 1xRTT service only facilitates SMS text messages[82] and a low rate data service as a backup to the

tracking device (as defined in section 3117 of this title [18 USCS § 3117]); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;").

77. *See* 18 U.S.C. § 2510(1) ("'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.;").

78. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 265-267.

79. *See* Telecommunications Industry Association, TIA-1157-A, *Signaling Conformance Test Specification for Interworking of CDMA2000 1X and High Rate Packet Data Systems, Revision A* (Arlington, VA: Aug. 2010), § 1.6, p. 1.2 ("Hybrid AT – An AT capable of operating on both a cdma2000 1x and HRPD system.").

80. *Id.*, § 1.2, p. 1.1.

81. By definition, cell phone hardware consists of "a compact speaker, a microphone, a keyboard, a display screen and a powerful circuit board with microprocessors." CTIA [website], *How Wireless Works*, http://www.ctia.org/consumer_info/index.cfm/AID/10324 (last accessed: Dec. 7, 2011).

82. "SMS: Short Messaging Service enables users to send and receive short text messages (usually about 140-160 characters) on wireless handsets. Usually referred to as 'text messaging' or 'texting.'" CTIA [website], Glossary of Terms Q-S, http://www.ctia.org/media/industry_info/

1xEV-DO Rel. 0 data service.

Each 1xEV-DO Rel. 0 Access Terminal has either an Electronic Serial Number (ESN) or Mobile Station Equipment Identifier (MEID) that uniquely identifies it among other Access Terminals and Mobile Stations.[83][84] The ESN consists of a unique 32-bit number[85] assigned to the wireless device by the manufacturer.[86] The ESN is stored on the Access Terminal's internal storage as a Permanent Access Terminal Indicator[87] and cannot be changed absent

index.cfm/AID/10406 (last accessed: Aug. 30, 2011).

83. *See* Telecommunications Industry Association, TIA-2000.5-D (Revision to TIA/IS-2000.5-C), *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems* (Arlington, VA: Mar. 2004), § 2.3.2, p. 2.6 ("The ESN or MEID is used to uniquely identify a mobile station in a wireless system.").

84. The majority of Access Terminals operating in 2008 had assigned ESNs. Newer Access Terminals have assigned MEIDs. Because there were/are so many wireless devices in existence, the wireless industry began to run out of unique assignable ESNs. *See* Telecommunications Industry Association, TIA-158, *Over-the-Air Service Provisioning for MEID-Equipped Mobile Stations in Spread Spectrum Systems* (Arlington, VA: Jan. 2005), § 1, p. 1.1. To fix this problem, the 56-bit MEID was introduced as the alternative to the ESN for new wireless devices. *See* TIA-158, *Over-the-Air Service Provisioning for MEID-Equipped Mobile Stations in Spread Spectrum Systems*, § 1, p. 1.1; Telecommunications Industry Association, TIA-1082, *MEID for cdma2000 Spread Spectrum Systems* (Arlington, VA: Sept. 2005), § 1.2, p. 1.2.

85. *See* Telecommunications Industry Association, *Electronic Serial Number Manufacturer's Code Assignment Guidlines And Procedures, Ver. 2.0* (Arlington, VA: Aug. 2008), *available at* http://ftp.tiaonline.org/wcd/WCD%20Meeting%20Sept.%204%202008/WCD-20080904-002_ESN_Guidelines_v2.0.pdf (last accessed: Feb. 20, 2012), p. 6.

86. *See id.*, p. 12 ("The ESN shall be factory set...").

87. *See* TIA-2000.5-D, *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems*, Annex F, § F.2.1, p. F.2 (Listing the ESN as a Permanent Mobile Station Indicator).

physical access to internal hardware.[88] Each Access Terminal has one or more internal electronic storage devices in the form of either an integrated memory chip or Removable User Identity Module (R-UIM).[89] A section of the Access Terminal's internal storage is called the Number Assignment Module (NAM)[90] used to store a copy of the ESN and the Mobile Identification Number (MIN).[91] In addition to storing the ESN and MIN, the NAM also stores other numeric indicators and parameters used for Access Terminal operation.[92] For example, among other categories of data, each Access Terminal NAM also stores: (1) the Preferred

88. *See* TIA, *Electronic Serial Number Manufacturer's Code Assignment Guidlines And Procedures, Ver. 2.0*, p. 7 ("The manufacturer will exercise due diligence in the design and manufacture of the MS to ensure that alteration of the factory set ESN is not possible outside of an authorized service center."); TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, Notes, p. xviii ("Each mobile station is assigned either a single unique 32-bit binary serial number (ESN) or a single unique 56-bit binary serial number (MEID) that cannot be changed by the subscriber without rendering the mobile station inoperative.").

89. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 214.

90. *See* CTIA [website], Glossary of Terms C-D, http://www.ctia.org/media/industry_info/index.cfm/AID/10321 (last accessed: Aug., 30, 2011) ("NAM (Number Assignment Module): The NAM is the electronic memory bank in the wireless phone that stores its specific telephone number and electronic serial number.").

91. *See* TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 1.2.1, p. 1.3 ("Mobile Identification Number (MIN). The 34-bit number that is a digital representation of the 10-digit number assigned to a mobile station."); *compare also id.* ("Mobile Directory Number. A dialable directory number which is not necessarily the same as the mobile station's air interface identification, *i.e.*, MIN, IMSI_M or IMSI_T.").

92. *See id.*, § 3.1, p. 3.1 ("The NAM indicators are parameters that can be assigned values using Over-the-Air Service Provisioning are specified in 4.5.2, 4.5.3, 4.5.4 and 4.5.6.").

Roaming List,[93] (2) the Extended Preferred Roaming List,[94] (3) Shared Secret Data (SSD),[95] [96] and (4) manufacturer-specific NAM parameters.[97] The numeric indicators and parameters stored on the NAM can be updated by the wireless carrier by writing and/or deleting data on the NAM via Over-the-Air Parameter Administration (OTAPA) or other similar methods.[98] *See Technical Explanations*, Section III(B)(3)(a), *infra*, for a full explanation of OTAPA. The four categories of NAM data listed above are further explained in proceeding subsections.

b. The Access Network (AN).

In order to provide data services to Access Terminals, a 1xEV-DO Rel. 0 cellular data network uses a set of hardware and software called the Access Network (AN). The Access

93. *See id.*, § 4.5.3, p. 4.38 *et seq.* (explaining the NAM Preferred Roaming List and Extended Preferred Roaming List parameter blocks); *id.*, § 3.5.5, p. 3.93 (Explaining the Preferred Roaming List and Extended Preferred Roaming List stored on the NAM).

94. *See* fn. No. 93, *supra*.

95. *See id.*, § 3.1, p. 3.1 ("The standard NAM indicators, stored in the mobile station's permanent and semi-permanent memory, are defined in F.3 of [1, 7]." (referring to TIA-2000.5-D)); *See* TIA-2000.5-D, *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems*, Annex F, § F.3, p. F.4 (Listing A-Key, Shared Secret Data A, and Shared Secret Data B as NAM indicators.).

96. *See* TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 3.5.8.14, p. 3.158 ([RE: reverse link] HRPD Access Authentication CHAP SS Parameters); *id.*, § 4.5.7.10, p. 4.56 ([RE: forward link] HRPD Access Authentication CHAP SS Parameters).

97. *See id.*, § 3.1, p. 3.1 ("Manufacturer-specific NAM parameters may be defined within a Parameter Block Type reserved for manufacturer-specific parameter definitions." (internal table references omitted)).

98. *See id.*, § 1.2.1, p. 1.4 ("Over-the-Air Parameter Administration (OTAPA). Network initiated OTASP process of provisioning mobile station operational parameters over the air interface.").

Network is responsible for providing "data connectivity between the packet-switched data network (typically the PDSN and Internet) and the ATs."[99] The Access Network is the equivalent of a Base Station (BS) in a 1xRTT network.[100] Both Access Networks and Base Stations are more commonly known as cell sites.[101][102] The Access Networks belonging to a 1xEV-DO Rel. 0 data network communicate with Access Terminals via radio waves transmitted through the air, *i.e.*, over the air interface. The radio waves sent between Access Terminals and Access Networks consist of signals that communicate data to/from the Access Terminal users and the Internet. A 1xEV-DO Rel. 0 Access Network consists of two main hardware/software elements: (1) the Base Transceiver Station (BTS),[103] and (2) the Base Station Controller[104] (BSC) which is sometimes "referred to as the radio network controller, or RNC."[105] "The BTS is an entity, composed of radio devices, antenna, and equipment, that provides

99. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 264-265.

100. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 1.11, p. 1.12 ("An access network is equivalent to a base station...").

101. In basic terms, a cell site is defined as "[t]he location where a wireless antenna and network communications equipment is placed in order to provide wireless service in a geographic area." CTIA [website], Glossary of Terms C-D, http://www.ctia.org/media/industry_info/index.cfm/AID/10321.

102. The remainder of the technical explanations contained in this section will refer to 1xEV-DO Rel. 0 cell sites as Access Networks when used in the context of 1xEV-DO Rel. 0 cellular data networks.

103. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 264, Fig. 10.23, "Basic network structure for 1X-EV DO."

104 *See id*.

105. *Id.*, p. 265.

transmission capabilities across the air interface (Um)."[106] In a 1xRTT network, "[t]he BSC is an entity that provides control and management for one or more BTSs and exchanges messages with its connected BTSs and the MSC [(*i.e.,* Mobile Switching Center)]."[107] In a 1xEV-DO network, the Base Station Controller (*i.e.*, the Radio Network Controller) performs the same function but instead of exchanging messages with a Mobile Switching Center, which is absent in a 1xEV-DO data network,[108] the BSC/RNC exchanges messages with (1) the "Access Network-Authentication, Authorization, and Accounting" (AN-AAA) server, and (2) the Packet Data Serving Node (PDSN).[109]

The first primary function performed by the BSC/RNC, exchanging messages with the AN-AAA server, is done to authenticate the Access Terminal to the Access Network and to collect data used for billing the wireless customer.[110] The AN-AAA authentication process, further explained in Section III(B)(3)(c)(vi), *infra*, prevents unauthorized wireless devices (*e.g.*, cloned wireless devices) from accessing data service through Access Networks while service is not authorized. Once the authentication process is complete, the BSC/RNC performs its second

106. *Id.*, p. 202.

107. *Id.* ("The MSC switches circuit-mode MS-originated or MS-terminated traffic and provides processing and control for calls and services.").

108. *See* Mishra, Ajay R., *Cellular Technologies for Emerging Markets: 2G, 3G and Beyond* (West Sussex, England: John Wiley & Sons, 2010), p. 113 ("...EV-DO uses an IP network and does not require a SS7 network and complex network switches such as a mobile switching center (MSC).").

109. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 266, Fig. 10.24, "Radio and core network interfaces protocols in 1X-EV DO."

110. *See id.*, p. 205 ("This function of AAA involves collecting and storing the billing-related data concerning the offered services...").

primary function, *i.e.*, exchanging data between the Access Network and the Packet Control Function (PCF),[111] which in turn relays the data to/from the Packet Data Serving Node[112] providing connectivity to the Internet.[113]

c. Access Networks (a.k.a. cell sites) in the geolocation context.

From a geolocation perspective, a 1xEV-DO Rel. 0 cellular data network provides service through a series of "cells" with each designating a geographical area located within the network coverage area.[114] Each cell, which is served by multiple cell **sites** (*i.e.*, Access Networks) pointing inward from the cell's borders, "is usually depicted as a hexagon, but in reality the actual shape varies according to the geographic environment and radio propagation."[115] A cell site in 1xEV-DO typically consists of three sets of multiple antennas, referred to as sectors, positioned atop an antenna tower, rooftop, or other structure allowing the

111. *See id.*, p. 204 ("The PCF is an entity... that manages the buffering and relay of packets between the BS and the PDSN.... The PCF also collects radio link (air interface)-related accounting information to be used by the AAA.").

112. *See id.*, p. 264, Fig. 10.23, "Basic network structure for 1X-EV DO."

113. *See id.*, p. 265 (The PDSN is "the network equipment providing data connectivity between the radio access network and a packet-switched data network. The PDSN provides connectivity to the Internet independent of the type of radio access network.")

114. *See* Chuah *et al.*, *Design And Performance Of 3G Wireless Networks And Wireless LANs*, p. 1 ("Today, the cellular systems consist of a cluster of base stations with low-power radio transmitters. Each base station serves a small cell within a large geographic area.").

115. *Id.*, p. 2.

antennas to operate across the earth's surface.[116][117] Cell site sectors "are created by installing multiple antenna sets at the base location, each with shielding on the 'back.' Each set of antennas is directional rather than omnidirectional."[118] The geographical signal coverage area of each sector depends on various factors such as power output of antenna amplifiers, antenna design,[119] and physical obstructions within the signal path area.[120] Sectors belonging to the

116. Although these "typical" cell sites are designed to cover relatively large sections of populated areas, other types of cell sites are becoming more common—even ones "designed to serve very small areas, such as particular floors of buildings or even individual homes and offices." Hearing Before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee On The Judiciary, House Of Representatives: *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of Matt Blaze, Associate Professor, University of Pennsylvania), p. 25, *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF (last visited: Jan. 5, 2012), p. 29.

117. The Verizon Wireless cell sites that were being accessed by the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.) were the typical tri-sectored type. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map of cell sites accessed by the aircard). Therefore, the remainder of this subsection will focus on the antenna design applicable to the actual Verizon Wireless cell sites accessed by the aircard in United States v. Rigmaiden.

118. Levine, *Digital Switching: Cellular & PCS Lectures April 17 & 24, 2001*, p. 11 ("Sectored cells have two advantages over omnidirectional cells. First, by limiting the radio reception/transmission to the 'front' of the angular sector and not transmitting or receiving a signal from the 'back' they reduce the level of interference by a ratio of 3/1 or 6/1 for 3 and 6 sectors, respectively. This improves the signal quality, which is manifested as a lower BER in a digital system.").

119. *See* Bedell, *Cellular/PCS Management: A Real World Perspective*, p. 38 ("Actual RF coverage is mainly determined by three key factors: the height of the cellular antenna (tower) at the base station, the type of antenna used at the cell base station, and the RF power level emitted.").

120. *See*, *e.g.*, CTIA [website], *How Wireless Works Pg 2,* http://www.ctia.org/consumer_info/index.cfm/AID/10539 (last accessed: Dec. 13, 2011)

most common type of cell site are positioned in a 360° circular formations with each sector covering an approximate 120° signal path area across the earth's surface.[121] The horizontal antenna angles designate the direction of each sector's 120° signal path area. In addition to having a physical location address (street address plus latitude and longitude), each cell site sector also has its own identification number. "This arrangement essentially divides the carrier's coverage area into a mosaic of local 'sectors', each served by an antenna at the nearest base station [(*i.e.*, cell site serving a cell)]."[122]

3. How relevant 3GPP2 technical standards dictate communications between a 1xEV-DO Rel. 0 Access Terminal and a 1xEV-DO Rel. 0 Access Network.

a. Over-the-Air Service Provisioning (OTASP) and Over-the-Air Parameter Administration (OTAPA).

As explained in Section III(B)(2)(a), *supra*, each Access Terminal NAM stores various data parameters such as the Preferred Roaming List, Extended Preferred Roaming List, Shared

("Since the shape and size or cells vary, there might also be empty spaces between the coverage areas of two or more cells. These gaps or dead spots can also be caused by trees, tall buildings or other obstructions that block your wireless signal from reaching a nearby antenna.").

121. *See* Levine, *Digital Switching: Cellular & PCS Lectures April 17 & 24, 2001*, p. 11 (diagram showing 120° tri-sectored cell site radiation pattern); *see also* O'Connor, Terrence P., *Provider Side Cell Phone Forensics*, Small Scale Digital Device Forensics Journal, Vol. 3, No. 1, June 2009 ISSN# 1941-6164, p. 1 ("The [][various] directional antennas on the cell tower nominally divide the 360 degree circumference around the tower into three 120 degree areas, one area for each antenna." (technical correction added in brackets)).

122. *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of Matt Blaze), p. 23 (PDF, p. 27) ("Network based location enables a cellular provider to identify the sector in which a user's [] [wireless device] is located, and, in some cases, to pinpoint their location within a sector.").

Secret Data (SSD), and manufacturer-specific NAM parameters.[123]—all of which can be surreptitiously updated by the wireless carrier through Over-the-Air Service Provisioning (OTASP).[124][125] OTASP is the process of reading,[126] writing,[127] and/or deleting[128] data to/from the internal storage device (*e.g.*, NAM) of an Access Terminal using commands sent by

123. The Preferred Roaming List, Extended Preferred Roaming List, and Shared Secret Data (SSD) are further explained in this subsection and in proceeding subsections.

124. *See* TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 1.1, p. 1.1 (listing features that can be provisioned over-the-air); *id.* § 3.3, p. 3.12 (listing programming procedures for OTASP).

125. Another method used by wireless carriers to update wireless devices over-the-air is IP Based Over-the-Air Device Management (IOTA-DM) using the Open Mobile Alliance Device Management (OMA DM) protocol. *See* 3rd Generation Partnership Project 2, 3GPP2 C.S0064-0, *IP Based Over-the-Air Device Management (IOTA-DM) for cdma2000 Systems, Release 0* (Sept. 6, 2012). "OMA DM provides an integrated and extensible framework for the OTA management needs of 3G mobile devices and beyond. The standard includes the OMA DM protocol specification, which is based on the SyncML DM protocol." *Id.*, § 1, p. 1.1 (internal citation omitted). "A method for updating firmware over the air (FOTA) based on OMA DM is also specified." *Id.* (citation omitted). "Firmware over-the-air (FOTA) is the process of **updating mobile station firmware over-the-air**. Primary use of firmware update capability is to rectify critical defects, that may compromise the end user safety, through updating firmware. It may be used to update new version of firmware to the mobile station." *Id.*, § 8, p. 8.1 (emphasis added). OMA DM is intended to replace OTASP but it is still backward compatible with the OTASP standard. *See id.*, § 1.4, p. 1.6 ("For backward compatibility with OTASP/OTAPA, the mobile and the server shall support converting IOTA-DM data to OTASP/OTAPA data." (internal citation omitted)).

126. *See* TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 3.5, p. 3.48 *et seq.* (explaining the data sent to Access Networks by Access Terminals via reverse link messages during OTASP).

127. *See id.*, § 4.5, p. 4.9 *et seq.* (explaining the data sent to Access Terminals by Access Networks via forward link messages during OTASP).

128. *See id*.

the Access Network to the Access Terminal over the air interface.[129] OTASP "allows a potential wireless service subscriber to activate (*i.e.*, become authorized for) new wireless service, and allows an existing wireless subscriber to make changes in existing services without the intervention of a third party [(*i.e.*, physical access to the user's device by a human)]."[130] OTASP can be initiated by either the Access Terminal or Access Network.[131] When initiated by the Access Network, the wireless carrier conducts Over-the-Air Parameter Administration (OTAPA)[132] to update the NAM or other operational parameters in the Access Terminal over-the-air.[133] "OTAPA sessions are initiated autonomously by the network, and proceed without any subscriber involvement or knowledge and with no limitation on the subscriber's ability to receive telecommunications services."[134] In order to read data from a specific NAM, the Access Network transmits a Configuration Request Message to the Access Terminal.[135] In

129. *See id.*, § 1.2.1, p. 1.4 ("Over-the-Air Service Provisioning (OTASP). A process of provisioning mobile station operational parameters over the air interface.").

130. *See* Telecommunications Industry Association, TIA-41.000-E-4[E], *Introduction to Mobile Application Part (MAP)* (Arlington, VA: Sept. 2007), § 3.1, p. 000.22.

131. TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 3.2, p. 3.2 ("Over-the-air service provisioning (OTASP) can be initiated in two ways: by the user and by the network.").

132. *See id.*, § 1.2.1, p. 1.4 ("Over-the-Air Parameter Administration (OTAPA). Network initiated OTASP process of provisioning mobile station operational parameters over the air interface."); *id.* § 3.2, p. 3.2 ("The network-initiated procedure... is also built upon the over-the-air programming protocol and procedures that support the OTASP feature.").

133. *See id.* § 3.2, p. 3.2 ("OTAPA provides a tool for the wireless service provider to update NAM indicators and parameters.").

134. *See* TIA-41.000-E-4[E], *Introduction to Mobile Application Part (MAP)*, § § 3.1, p. 000.21.

135. *See* TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread*

response to the Configuration Request Message, the Access Terminal transmits a Configuration Response Message providing the Access Network with its stored NAM parameters.[136] In order to write data to an Access Terminal NAM, the Access Network transmits a Download Request Message containing the NAM parameter blocks sought to be written.[137] In order to cause the Access Terminal to commit the parameter blocks to permanent NAM memory, the Access Network transmits a Commit Request Message to the Access Terminal.[138] A newly purchased Access Terminal will receive an initial NAM provisioning[139] and, throughout the course of service, the Access Network will periodically update the data stored on the NAM via OTAPA according to relevant protocols.

Prior to reading, writing, and/or deleting data to/from an Access Terminal NAM, the Access Network must first complete SPC/SPL and SPASM security procedures to unlock and gain access to the NAM. The Service Programming Code (SPC)[140] and Service Programming Lock (SPL) parameter[141] contained on the NAM "prevents the over-the-air provisioning of

Spectrum Systems, § 3.3.1, p. 3.12-3.13.

136. *See id*.

137. *See id.*, § 3.3.1, p. 3.13-3.14.

138. *See id.*, § 3.3.1, p. 3.14-3.16.

139. *See id.*, § 4.2.1, p. 4.1.

140. *See id.*, § 1.2.1, p. 1.5 ("Service Programming Code (SPC). A secret code assigned to the mobile station and known to the authorized network entity.")

141. *See id.* ("Service Programming Lock (SPL). A protection provided for preventing the over-the-air provisioning of certain mobile station parameters by unauthorized network entity by way of verifying the Service Programming Code (SPC).").

certain mobile station parameters by an unauthorized network entity."[142] The SPL parameter contains the SPC, taking a numeric value of 1 to 999,999,[143] "used for unlocking the mobile station parameters for programming or reprogramming."[144] Due to the weak security of the SPC/SPL "combination lock" type mechanism,[145] an Access Terminal NAM also uses the Subscriber Parameter Administration Security Mechanism (SPASM). SPASM serves the same purpose as SPC/SPL[146] but, instead of a simple numeric code, SPASM utilizes the Shared Secret Data (SSD) stored on the NAM and known only to the Access Terminal and home AN-AAA server.[147] SPASM uses cryptographic keys and mathematical equations to conduct a type of challenge-response between the Access Terminal and Access Network so that the Access Terminal can verify that it is having its NAM provisioned by an authorized entity.[148]

Most commonly, the wireless carrier uses OTAPA to set the NAM's Preferred Roaming List and Extended Preferred Roaming List with values that (1) designate which radio frequencies to scan in order to acquire a system (*i.e.*, groups of wireless carrier cell sites), and

142. *Id.*, § 1.1, p. 1.1.

143. *Id.*, § 3.3.6, p. 3.43, Table 3.3.6-1 (Service Programming Code Values).

144. *Id.*, § 3.3.6, p. 3.42.

145. A numeric security code or combination having only 999,999 possible values is susceptible to a "brute force" attack, *i.e.*, a security code "guessing" attack.

146. *See id.*, § 1.2.1, p. 1.5 ("Subscriber Parameter Administration Security Mechanism (SPASM). Security mechanism protecting parameters and indicators of active NAM from programming by an unauthorized network entity during the OTAPA session.")

147. *See id.*, § 3.3.7, p. 3.43 (explaining how SPASM works).

148. *See id*.

(2) designate which systems are authorized for providing service.[149] "The preferred roaming list consists of two tables: the system table and the acquisition table."[150] The Acquisition Table lists Acquisition Records consisting of "parameters that the mobile station can use to acquire a system. Each type of acquisition record is tailored for use in acquiring a particular kind of system."[151] The System Table lists System Records containing "parameters that the mobile station can use for identifying an acquired system, for determining whether an acquired system is the optimal system on which to operate and for determining the mobile station's roaming status."[152] In basic terms, the Acquisition Table contains a list of radio frequencies[153] the Access Terminal may scan in order to locate transmitting Access Networks,

149. "Two categories of the preferred roaming list are defined: The Preferred Roaming List and the Extended Preferred Roaming List." *Id.*, § 3.5.5, p. 3.93. When accessing 1xEV-DO Access Networks, a High Rate Packet Data (HRPD) (*i.e.*, 1xEV-DO) Access Terminal uses its *Extended* Acquisition Records and *Extended* System Records contained in its *Extended* Preferred Roaming List. *See id.*, § 3.5.5.3.2, p. 3.114-3.120 and 3.5.5.2.2.11, p. 3.112. However, because the Extended Preferred Roaming List is considered a category of the Preferred Roaming List (*see id.*, § 3.5.5, p. 3.93), the "Extended" prefix will be omitted and the terms "Preferred Roaming List," "Acquisition Table," "Acquisition Record," "System Table," and "System Record" will be used from this point forward for sake of simplicity.

150. *Id.*, ANNEX C, p. C.1.

151. *Id.*, § 3.5.5.2, p. 3.98.

152. *Id.*, § 3.5.5.3, p. 3.112.

153. *See id.*, § 3.5.5.2.2.11, p. 3.112 (Generic Acquisition Record for HRPD (*i.e.*, 1xEV-DO Rel. 0) containing band-class and channel number).

and the System Table contains a list of HRPD IPv6[154] subnets[155] acting as unique identification numbers for groups of Access Networks (*i.e.*, systems) authorized for providing service.[156] In addition to the subnet information identifying a system, each record in the System Table also contains "an indicator of whether the system is preferred or negative, the roaming status that should be indicated by the mobile station, the relative priority of the system and its geographic region."[157] "The records in the acquisition table are in order of priority (highest priority first) according to desired mobile station system selection scan order."[158]

b. Access Terminal Initialization State procedures: identifying and acquiring a 1xEV-DO Rel. 0 Access Network after initial power-on.

The first step of identifying and acquiring an Access Network is to place the Access

154. In 1xEV-DO Rel. 0, Access Network sectors are identified by 128-bit Internet Protocol Version 6 (IPv6) addresses. *See* TIA-856-2[E], *cdma2000 High Rate Packet Data Air Interface Specification – Addendum 2*, § 10.9, p. 10.11 (section from more recent version of IS-856 covering "SectorID Provisioning"); *see also* IETF RFC 2373, *IP Version 6 Addressing Architecture*. The subnet corresponding to any given Access Network IPv6 address identifies the system to which the Access Network belongs. In other words, the 1xEV-DO subnets take the place of the System Identification numbers (SIDs) and Network Identification numbers (NIDs) used to identify groups of cell sites.

155. *See id.*, § 3.5.5.3.2-3.5.5.3.2.1, p. 3.118-3.20 (indicating that the system ID record for HRPD (*i.e.*, 1xEV-DO Rel. 0) System Table contains the following data fields used to deduce the IPv6 subnet identifying the 1xEV-DO system: SUBNET_COMMON_INCLUDED, SUBNET_LSB_LENGTH, SUBNET_LSB, SUBNET_COMMON_OFFSET, SUBNET_COMMON_LENGTH, and SUBNET_COMMON.).

156. *See Technical Explanations*, Section III(B)(3)(c)(i), *infra* (explaining use of the System Table).

157. *See TIA-683-D, Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, ANNEX C, p. C.1.

158. *Id*.

Terminal into the Initialization State by powering it on.[159] In the case of an aircard, this is accomplished by plugging the device into the PCMCIA slot of a host laptop computer. Once plugged in, the Access Terminal receives power from the laptop's power source and its radio transceiver is automatically initiated. Once powered on, the Access Terminal is considered to be in the Inactive Substate of the Initialization State.[160] Prior to any interaction by the human user, the Access Terminal begins the process of identifying radio signals belonging to available Access Networks[161] authorized to provide 1xEV-DO Rel. 0 data service. In order to accomplish this task, the Access Terminal hardware transitions out of the Inactive Substate and into the Network Determination Substate.[162]

i. Network Determination Substate.

While in the Network Determination Substate, "the access terminal selects a CDMA Channel on which to try and acquire the access network."[163] Considering Access Networks can transmit on any number of radio frequencies,[164] the Access Terminal must first select a

159. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.2.6.1.2.1, p. 6.12 ("The access terminal shall enter the Initialization State when the Default Air-Link Management Protocol is instantiated. This may happen on events such as network redirection and initial power-on.")

160. *See id.*, § 6.3.1, p. 6.18 ("In this state the protocol waits for an *Activate* command.").

161. *See id.*, § 6.2.6.1.2, p. 6.11 ("In the Initialization State the access terminal has no information about the serving access network. In this state the access terminal selects a serving access network and obtains time synchronization from the access network.").

162. *See id.*, § 6.3.1, p. 6.18 ("Network Determination State: In this state the access terminal chooses an access network on which to operate.").

163. *See id.*, § 6.3.6.1.3, p. 6.22 (internal reference omitted).

164. *See id.*, § 9.2.1.1.1, p. 9.6 *et seq.* (Channel Spacing and Designation).

frequency to monitor using its Preferred Roaming List[165] (stored on the Access Terminal NAM) through a process called System Selection for Preferred Roaming (SSPR). "The goal of System Selection for Preferred Roaming (SSPR) is for the mobile station to acquire the most preferred system using the information from the preferred roaming list [] stored in the mobile station [].";[166] As previously explained, "[t]he preferred roaming list consists of two tables: the system table and the acquisition table."[167] While in the Network Determination Substate, the Access Terminal initiates System Selection for Preferred Roaming (SSPR) by reading from the Acquisition Table to obtain either CDMA frequency blocks or specific CDMA channels within frequency blocks of which to scan for available Access Networks.[168] In the case of 1xEV-DO Rel. 0 or other High Rate Packet Data (HRPD) service, the Acquisition Table will have one or more "Generic Acquisition Record for HRPD" consisting of a "Band Class number corresponding to the frequency assignment of the channel" and a "channel number corresponding to the Band Class[.]"[169] The various Preferred Roaming List "Generic Acquisition Record for HRPD" entries are listed according to selection preference.[170] The

165. *See* TIA-683-D, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 1.2.2, p. 1.7 ("PR_LIST s-p - Preferred Roaming List. Contains information to assist the mobile station system selection and acquisition process. Retained by the mobile station when the power is turned off.").

166. *See id.*, § 3.3.5, p. 3.42 (internal reference and NAM indicator name omitted).

167. *Id.*, ANNEX C, p. C.1.

168. *See id.*, § 3.5.5.2.1, p. 3.100 *et seq.* (listing Acquisition Record Formats).

169. *See id.*, § 3.5.5.2.2.11, p. 3.112.

170. *See id.*, § 3.5.5.2, p. 3.100 ("If ACQ_TABLE contains more than one acquisition record, these records should be listed in priority order (highest priority first) according to the desired

Access Terminal will begin by selecting the entry having the highest preference and then it will copy the relevant channel(s) to be scanned into a temporary Channel Record maintained on its internal storage.[171] Once the Access Terminal makes a Channel Record, it transitions from the Network Determination Substate to the Pilot Acquisition Substate.[172]

ii. Pilot Acquisition Substate.

"In the Pilot Acquisition S[ubs]tate the access terminal acquires the Forward Pilot Channel of the selected CDMA Channel."[173] The pilot channel is an "unmodulated direct sequence spread spectrum signal continuously transmitted at a fixed power"[174] by each Access Network sector. The pilot channel "is continually transmitting an all zero signal, which is covered by a Walsh code 0,"[175] and is only identifiable because the "all-zero baseband stream is [] multiplied by a pair of quadrature PN sequences."[176] Because of the all-zero baseband

mobile station system selection scanning priorities.").

171. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.3.6.1.3, p. 6.22 ("In the Network Determination State the access terminal selects a CDMA Channel (see 10.1) on which to try and acquire the access network."); § 10.1, p. 10.1 ("The Channel record defines an access network channel frequency and the type of system on that frequency.").

172. *See id.*, § 6.3.6.1.3, p. 6.23 ("Upon selecting a CDMA Channel the access terminal shall enter the Pilot Acquisition State.").

173. *Id.*, § 6.3.6.1.4, p. 6.23.

174. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 38.

175. Langton, Charan (complextoreal.com), *CDMA Tutorial: Intuitive Guide to Principles of Communications* (2002), *available at* http://www.complextoreal.com/CDMA.pdf (last accessed: Sept. 29, 2010), p. 12; *see also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 235 ("The pilot channel carries all '0's, that is, no upper layer information.").

176. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 39.

stream, "the pilot channel has very good SNR [(Signal to Noise Ration)] making it easy for mobiles to find it."[177] "The pilot is the first broadcast physical channel that is searched and acquired by the mobile stations immediately after the mobile is powered on."[178] "The main functions of the pilot channel [in 1xEV-DO Rel. 0] are the same [as] those of forward common pilot channels in cdma2000 or IS95."[179] The pilot channel is used to broadcast a unique signature (etymologically referred to as a PN sequence, short code, PN offset, or PN code) used by Access Terminals to identify and differentiate between all Access Network sectors in a given area. "The PN sequence, with a specific offset, forms a short code, which uniquely identifies the pilot and thereby the particular sector that is transmitting that pilot signal."[180] Each CDMA transmit frequency, corresponding to a band class CDMA channel number, supports a total of 512 unique PN sequences of which short codes can be derived for any given area.[181]

In addition to using the short code to identify the Access Network, the Access Terminal also uses the short code to identify and decode all other forward link radio channels transmitted by the Access Network. This is required because the Access Network uses the short code "to

177. Langton, *CDMA Tutorial: Intuitive Guide to Principles of Communications*, p. 12; *see also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 39 ("As a result, the pilot is an easy-to-capture signal, which mainly reflects the phase of the PN sequence used as the base station's short code.").

178. *Id.*, p. 38.

179. *Id.*, p. 235.

180. *Id.*, p. 39.

181. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.3.1.3.4, p. 9.90 ("Pilot Channels shall be identified by an offset index in the range from 0 through 511 inclusive.").

spread [(*i.e.*, encode)] the composite signal (containing all code channels) that is transmitted to the users in a cell."[182] "[T]he base station-specific short codes serve as the base stations' signatures, allowing differentiation and de-spreading of desired base stations' signals in the presence of other-cell interference."[183] Aside from physical layer identification and decoding, the Access Terminal also uses the "power and timing of the pilot channel"[184] to simplify the determination of the best serving Access Network[185] and to help in "acquiring the system timing and fast synchronization."[186][187] Although the pilot channel does not transmit system time, the nature of the PN sequence transmission[188] allows the Access Terminal to synchronize

182. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 18; *see also* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.3.1.3.1, p. 9.60 fig. 9.3.1.3.1-1, "Forward Channel Structure" (showing composite Walsh channels labeled "A" and "B" being fed into the Quadrature Spreading block prior to output of Forward Modulated waveform).

183. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 31-32.

184. *Id.*, p. 235.

185. *See id.*, p. 249 ("The AT uses the measured SINR [(Signal to Interference and Noise Ration)] of the strongest pilot and the thresholds defined by the AN to determine the highest data rate it can reliably decode as well as the identity of the corresponding best serving sector.").

186. *Id*.

187. "An additional function of the pilot [(specific to 1xEV-DO)] is to provide the access terminal with a means of predicting the receive C/I for the purpose of access-terminal-directed forward data rate control (DRC) of the Data Channel transmission." TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.3.1.3.1, p. 9.56 fn. 54.

188. *See id.*, § 9.3.1.3.4, p. 9.90 ("The chip rate for the pilot PN sequence shall be 1.2288Mcps. The pilot PN sequence period is 32768/1228800 = 26.666… ms, and exactly 75 pilot PN sequence repetitions occur every 2 seconds."); *id.* ("The zero-offset pilot PN sequence shall be such that the start of the sequence shall be output at the beginning of every even second in time, referenced to access network transmission time.").

its clock ticks to the clock ticks of the Access Network.[189] This synchronization is required because all forward link channels are placed into time slots "aligned to the PN rolls of the zero-offset PN sequences and... to system time on even-second ticks."[190]

"Upon entering the Pilot Acquisition S[ubs]tate, the access terminal shall tune to the selected CDMA Channel and shall search for the pilot."[191] If the Access Terminal is unable to acquire at least one pilot signal from the selected CDMA channel within a set amount of time, the Access Terminal makes a new channel record using the next highest priority entry from the Preferred Roaming List Acquisition Table.[192] For example, assume a scenario where the highest priority entry in the Acquisition Table contains a band class and channel number equating to 880.020−880.650 MHz radio frequency for the Access Network and the second highest priority entry in the Acquisition Table contains a band class and channel number equating to 891.510−893.370 MHz radio frequency for the Access Network. Under this scenario, the Access Terminal will first monitor 880.020−880.650 MHz for a pilot signal and if no pilot is detected, the Access Terminal will then monitor 891.510−893.370 MHz for a pilot signal. This process will continue for each entry in the Acquisition Table of the Preferred

189. In other words, the noted synchronization causes the "second hand" of the Access Terminal's internal clock to tick in unison with the "second hand" of the Access Network's internal clock but the absolute system time is still unknown to the Access Terminal.

190. *Id.*, § 9.3.1.3.1, p. 9.57; *see also id.*, § 9.3.1.3.6.1, p. 9.93 ("Each sector shall use a time base reference from which all time-critical transmission components, including pilot PN sequences, slots, and Walsh functions, shall be derived.").

191. *Id.*, § 6.3.6.1.3, p. 6.23.

192. *See id.* ("If the access terminal fails to acquire the pilot within [][a specified amount of] seconds of entering the Pilot Acquisition State, it shall enter the Network Determination State.").

Roaming List until an initial Access Network pilot signal is detected.[193] Once the Access Terminal has acquired the pilot channel, derived the short code, and synchronized its clock ticks to the system timing, it transitions out of the Pilot Acquisition Substate and into the Synchronization Substate.[194]

iii. Synchronization Substate.

In the Synchronization Substate, "the access terminal synchronizes to the Control Channel cycle, receives the Sync message, and synchronizes to system time."[195] In 1xEV-DO Rel. 0, the Sync message is transmitted on the Control Channel,[196] a forward link traffic channel, which takes the place of the Sync Channel used in 1xRTT and in other earlier CDMA communications systems.[197] "The access network broadcasts the Sync message to convey basic network and timing information."[198] The "broadcast" addressing for the Sync message means all Access Terminals are sent the same Sync message at the same time.[199] The Access

193. Through the Route Update Protocol, additional pilot signals for additional Access Network sectors are detected and logged after the Access Terminal acquires the initial Access Network. The details of this process are explained in the *Technical Explanations*, Section III(B)(3)(d)(i), *infra*.

194. *See id.*, § 6.3.6.1.4, p. 6.23 ("If the access terminal acquires the pilot, it shall enter the Synchronization State." (footnote omitted)).

195. *See id.*, § 6.3.1, p. 6.18.

196. *See id.*, § 6.3.6.1, p. 6.22 ("The access network shall broadcast the Sync message periodically in a synchronous Control Channel capsule.").

197 *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 39 (discussing the Sync Channel in IS-95A) & p. 144 (discussing the Sync Channel in 1xRTT).

198. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.3.6.2.1, p. 6.23.

199. *See id.* (the "addressing" table entry is set to "broadcast" for the Sync message) & §

Network uses the Sync message to write network specific data to the internal storage devices of all Access Terminals attempting to acquire the network. In 1xEV-DO, the Sync message contains five parameters (*i.e.*, data fields) sent to the Access Terminal: (1) MessageID, (2) MaximumRevision, (3) MinimumRevision, (4) PilotPN, and (5) SystemTime.[200][201] Upon receiving the Sync message, the Access Terminal "reads and stores all the parameters in the message that are defined in the mobile protocol revision and ignores the rest."[202] After storing the data contained in the Sync message, the Access Terminal checks to see if its protocol revision number is between the MinimumRevision and MaximumRevision fields of the Access Network.[203] If the Access Terminal's revision number is not within the specified range then the Access Terminal and Access Network are not compatible and the Access Terminal transitions back to the Network Determination Substate.[204] If the Access Terminal's revision number is within the specified range then the Access Terminal and Access Network are compatible and the Access Terminal sets its "time to the time specified in the message[.]"[205]

6.3.6.1, p. 6.22 ("The access network shall broadcast the Sync message periodically in a synchronous Control Channel capsule.").

200. Unlike the pilot signal that provides clock tick synchronization, the SystemTime parameter of the Sync message provides the Access Terminal with an absolute system time value.

201. *See id.* § 6.3.6.2.1, p. 6.24.

202. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 144.

203. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.3.6.1.5, p. 6.23.

204. *See id*.

205. *Id.*, § 6.3.6.1.5, p. 6.23.

At this point, the Access Terminal has acquired the network and transitions out of the Initialization State[206] and into the Idle State.

c. Access Terminal Idle State procedures: preparing to open a connection and opening a connection with a 1xEV-DO Rel. 0 Access Network.

While in the Idle State, the Access Terminal's actions are primarily dictated by the Default Idle State Protocol, which "provides the procedures and messages used by the access terminal and the access network when the access terminal has acquired a network and a connection is not open."[207] There are seven primary functions performed by the Access Terminal while in the Idle State:[208] (1) receiving, processing, and storing to internal storage the Access Network's Overhead Messages, (2) transmission of Access Probes to the Access Network to initiate session establishment and open a connection, (3) establishing an open session with the Access Network, (4) application of encryption and authentication keys for use in the security layer, (5) obtaining identifying information from Access Terminal hardware using the HardwareIDRequest message, and (6) opening a connection with the Access Network. The above listed functions are fully explained in the subsections immediately below.

206. Inactive, Network Determination, Pilot Acquisition, and Synchronization were all substates of the Initialization State.

207. *Id.*, § 6.4.1, p. 6.26.

208. There are other functions relevant to this state but, unless otherwise noted in later subsections, they are immaterial to the operation of the FBI's cell site emulators (as used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.)) and will not be addressed.

i. Receiving, processing, and storing to internal storage the Access Network's Overhead Messages.

Upon entering the Idle State, the Access Terminal is in an Inactive Substate and proceeds into the Monitor Substate. "When the access terminal is in the Monitor S[ubs]tate, it continuously monitors the Control Channel."[209] In this substate, "[t]he access terminal shall monitor the overhead messages as specified in the Overhead Messages Protocol []."[210] The Overhead Messages are the QuickConfig message and the SectorParameters message.[211] "These messages are broadcast by the access network over the Control Channel."[212] The "broadcast" addressing for the Overhead Messages means all Access Terminals are sent the same Overhead Messages at the same time.[213] The QuickConfig and SectorParameters messages contain numerous categories of essential data communicated to Access Terminals.[214] [215] "The QuickConfig message is used to indicate a change in the overhead messages'

209. *Id.*, § 6.4.6.1.5, p. 6.35.

210. *Id.*, § 6.4.6.1.5.1, p. 6.35.

211. *See id.*, § 6.8.1, p. 6.113.

212. *Id*.

213. *See* 6.8.6.1.5, p. 6.118.

214. *See id.*, § 6.8.6.2.1, p. 6.120 (Listing the following data fields for the QuickConfig message: MessageID, ColorCode, SectorID24, SectorSignature, AccessSignature, Redirect, RPCCount, ForwardTrafficValid, and a Reserved field.).

215. *See id.*, § 6.8.6.2.2, p. 6.122 (Listing the following data fields for the SectorParameters message: MessageID, CountryCode, SectorID, SubnetMask, SectorSignature, Latitude, Longitude, RouteUpdateRadius, LeapSeconds, LocalTimeOffset, ReverseLinkSilenceDuration, ReverseLinkSilencePeriod, ChannelCount, Channel, NeighborCount, NeighborPilotPN, NeighborChannelIncluded, NeighborChannel, NeighborSearchWindowSizeIncluded, NeighborSearchWindowSize, NeighborSearchWindowOffsetIncluded, NieghborSearchWindowOffset, and a Reserved field.).

contents and to provide frequently changing information."[216] "The SectorParameters message is used to convey sector specific information to the access terminals."[217] The Access Network uses the Overhead Messages to write network specific data to the internal storage devices of all Access Terminals that have acquired the network but are yet to establish a connection. "When a mobile station receives an overhead message, it should update all of its related stored information accordingly."[218] The Access Terminal will also "store the signature associated with the message for future comparisons."[219] By comparing the signature of the previous Overhead Message to the signature of the new Overhead Message, the Access Terminal can determine if it needs to update its stored data sent to it by the Access Network.[220] The Overhead Message parameters written to the Access Terminal by the Access Network are "essential parameters" that are "shared by protocols in the Connection Layer as well as protocols in other layers."[221]

Immediately after receiving the SectorParameters message, the Access Terminal uses the SectorID and SubnetMask[222] data parameters to determine the subnet of the system to which

216. *Id.*, § 6.8.6.2.1, p. 6.120.

217. *Id.*, § 6.8.6.2.2, p. 6.121.

218. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 153.

219. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.8.6.1.6, p. 6.119.

220. *See id.*, § 6.8.6.1.6, p. 6.118 (explaining the signature comparison process).

221. *Id.*, § 6.1.1, p. 6.2.

222. *See id.*, § 1.11, p. 1.15 (Explaining the IPv6 SubnetMask to be "[a] 128-bit value whose binary representation consists of *n* consecutive '1's followed by 128-*n* consecutive '0's.").

the Access Network belongs. The SectorID of the SectorParameters message contains a 128-bit Internet Protocol Version 6 (IPv6) address that identifies the sector.[223] The SubnetMask of the SectorParameters message contains "the number of consecutive 1's in the subnet mask of the subnet to which th[e] sector belongs."[224] In order to calculate the IPv6 subnet from the SectorParameters message, the Access Terminal conducts a mathematical bitwise logical AND using the SectorID and the SubnetMask.[225] As explained in Section III(B)(3)(a), *supra*, the subnet of the serving sector acts as the unique identification number identifying the particular 1xEV-DO system being accessed by the Access Terminal. No two 1xEV-DO systems have the same subnet and all Access Networks belonging to any given system will have identical subnet values as calculated using the SectorID and SubnetMask. Once the Access Terminal deduces the subnet of the serving system, it checks its locally stored Preferred Roaming List System Table[226] to determine if the subnet is listed as corresponding to a group of Access Networks (*i.e.*, a system) authorized for providing wireless service. If the subnet is not authorized, the

223. *See id.*, § 6.8.6.2.2, p. 6.123 (Defining the SectorID as the "Sector Address Identifier[]" and that "[t]he access network shall set this field to the 128-bit IPv6 address of th[e] sector." (internal citation omitted)); *see also* IETF RFC 2373, *IP Version 6 Addressing Architecture*.

224. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.8.6.2.2, p. 6.123.

225. *See* Becker, Ralph, IP Address Subnetting Tutorial (Sept. 7, 1999), *available at* http://www.firstnetsecurity.com/library/misc/TutorialMaster.PDF (last accessed: Feb. 20, 2012) (explaining IPv4 subnetting techniques); DSLReports.com, [website], *How to Calculate the Subnet of an ip for your network. IPv6 FAQ | DSLReports.com, ISP Information*, http://www.dslreports.com/faq/16362 (last accessed: Feb. 20, 2012) ("To subnet the IPv6 address space, you use same ipv4 subnetting techniques to divide... different portions of an IPv6 intranet.").

226. *See Technical Explanations*, Section III(B)(3)(a), *supra* (explaining the Preferred Roaming List System Table and its purpose).

Access Terminal ignores the Access Network and transitions back to the Network Determination Substate. If the subnet is authorized, the Access Terminal begins the access probe process to initiate session establishment with the Access Network.

ii. Transmission of Access Probes to the Access Network to initiate session establishment and open a connection.

Prior to the initial Access Probe process explained in this subsection, all radio signal transmissions are broadcast by the Access Network to the Access Terminal. Immediately after network acquisition, the Access Terminal is yet to transmit signals and the Access Network is yet to be made aware of the Access Terminal's presence.[227] In order to establish a session and open a connection with the Access Network, the Access Terminal initiates an Access Attempt over the Reverse Access Channel belonging to the sector serving the Access Terminal.[228] "Each access attempt may consist of one or more sub-attempts, each consisting of repeated transmissions of the same message. Each message transmission is called an *access probe*."[229] All Access Channel transmissions are spread (*i.e.*, encoded)[230] using a long code created from

227. *See id.*, p. 52 ("When the mobile first attempts to access the system, the base station has no information about the location of the mobile...").

228. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.3.2, p. 9.33 ("The Access Channel is used by the access terminal to initiate communication with the access network...).

229. *See* Korowajczuk, Leonhard *et al.*, *Designing cdma2000 Systems*, John Wiley & Sons, (West Sussex, England: 2004), p. 254; *see also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 247 ("The transmissions on the access channel are in the form of access probes, each consisting of a preamble followed by one or more access channel physical layer packets." (internal figure note omitted)).

230. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 8.3.6.1.4.1.1, p. 8.25 ("The access terminal shall use the Access Channel long codes to cover the entire probe.").

stored data received via the Overhead messages.[231][232] A 1xEV-DO Access Probe transmission "consist[s] of a preamble followed by one or more access channel physical layer packets."[233] "During the preamble transmission, only the Pilot Channel is transmitted."[234] "During the Access Channel physical layer packet transmission, both the Pilot Channel and the Data Channel are transmitted."[235] The physical layer packet transmissions contain higher layer Protocol Data Units[236] used for establishing a session and opening a connection with the Access Network.[237] A transmission sent on the Access Channel by the Access Terminal is always part of an Access Attempt dictated by the Access Probe process.

231. *See id.*, § 8.3.6.1.4.1.2, p. 8.26, Table 8.3.6.1.4.1.2-1, Access Channel Long Code Masks (showing that the long code mask for the Access Channel is comprised, in part, by the ColorCode and SectorID); *id.*, § 8.3.6.1.4.1.2, p. 8.27 ("SectorID is given as public data of Overhead Messages Protocol and corresponds to the sector to which the access terminal is sending the access probe. [] ColorCode is given as public data of Overhead Messages Protocol and corresponds to the sector to which the access terminal is sending the access probe.").

232. The entire forward link channel, which includes the Access Channel spread by the Access Channel long code, is also collectively spread by the Access Network short code as explained in the *Technical Explanations*, Section III(B)(3)(b)(ii), *supra*.

233. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 247 (internal figure note omitted).

234. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.3.2, p. 9.33; *see also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 33 ("The preamble does not carry any m[e]ssages and it is transmitted to help [the] base station capture the phase and timing of [the] user's transmission in the uplink. Once the preamble is detected the base station can demodulate the message capsule and process [the] MS's request.").

235. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.3.2, p. 9.33-9.34.

236. *See id.*, § 8.3.3, p. 8.18 (defining the Protocol Data Unit for the Default Access Channel MAC Protocol).

237. *See id.*, § 8.3.6.1, p. 8.21 and Fig. 8.3.6-1. Access Channel MAC Packet Structure.

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

In 1xEV-DO, "[t]he access procedure performed by the access channel MAC protocol is similar to that used in basic access mode of IS-2000."[238] "Namely, the AT keeps transmitting access probes at increasing power levels until it gets an acknowledgement back from the AN."[239] The 1xEV-DO Access Probe process adopted from earlier CDMA technology solves the power control[240] problem inherent with initial reverse link transmissions: "When the mobile first attempts to access the system, the base station has no information about the location of the mobile and thus the power at which the mobile should access the system"[241] An Access Attempt involves transmitting Access Probes "starting with a low initial power estimated by open-loop power control followed by power increments on every successive

238. Yang, Samuel C., *3G CDMA2000: Wireless System Engineering* (Norwood, MA: Artech House, 2004) p. 229; *see also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 247 ("In 1X-EV DO the access channel structure and protocols are very similar to those of IS95/cdma2000 Release 0.").

239. Yang, *3G CDMA2000: Wireless System Engineering*, p. 229; *see also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 52 ("The mobile attempts to access the system by transmitting a series of access probes. The first access probe is transmitted at a relatively low power and is followed by a series of successive probe transmissions of progressively higher power until an acknowledgment is received.").

240. 1xEV-DO and other CDMA based technologies are dependent on strict power control across the various transceivers making up the network. *See*, *e.g.*, Levine, *Digital Switching: Cellular & PCS Lectures April 17 & 24, 2001*, p. 58 ("When multiple transmitters send signals with different PN codes to a common receiver, the RSSI of all the signals must be very close to equal, or the strongest one will dominate all the others and only it can be decoded without errors. This was a major problem which caused malfunctions of a trial CDMA system used in tests by the Groupe Spécial Mobile in 1986 in Paris. Qualcomm revived the idea of CDMA for cellular in 1989 with an improved closed- loop feedback power control to keep all the received signals from deviating in individual power levels.").

241. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 52.

probe within an access attempt."[242] "Similar to IS95 and cdma2000, the access terminal sends a series of access probes until it receives a response from the access network or the timer expires."[243] "The transmission of request or response messages through the air interface does not assure successful access to the system. The process is only complete after the same message is sent a certain number of times or when the MS receives a reception acknowledgement (ACK)."[244] In other words, the Access Terminal transmits the same message over and over, each time increasing the transmission power, until the Access Network responds with an acknowledgement that the message was received. Once the Access Terminal receives the acknowledgement, it will begin transmitting the next message using the same Access Probe process. As long as the Access network continues to respond to Access Probes, the process will continue until the Access Attempt is successfully completed (*i.e.*, a session is established and a connection is open).

Before the Access Terminal can begin transmitting Access Probes, it first needs to receive and process the AccessParameters message[245] broadcast by the Access Network.[246]

242. *Id.*, p. 247.

243. *Id*.

244. Korowajczuk, *Designing cdma2000 Systems*, p. 254; *see also* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 8.3.3.6.1.4.1.1, p. 8.25 ("The access terminal shall not change the probe data contents in between probes.").

245. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 8.3.6.1.4.1.1, p. 8-25 ("Prior to sending the first probe of the probe sequence, the access terminal shall verify that the last AccessParameters message it received is current...").

246. *See id.*, § 8.3.6.2.6, p. 8-33 (the "addressing" table entry is set to "broadcast" for the AccessParameters message).

The "broadcast" addressing for the AccessParameters message means all Access Terminals are sent the same message at the same time. The Access Network uses the AccessParameters message to write network specific data to the internal storage devices of all Access Terminals that are attempting to access the network after network acquisition.[247] The AccessParameters message contains numerous categories of essential data communicated to Access Terminals for use in power control and formatting of Access Probe transmissions.[248] Upon receiving the AccessParameters message, the Access Terminal reads and stores all data fields contained in the message. The Access Terminal uses the stored data fields,[249] along with stored data fields from the Overhead Messages,[250] to configure Access Probe transmissions and to facilitate Access Attempts.[251]

247. *See id.*, § 8.3.6.2.6, p. 8-31 ("The AccessParameters message is used to convey Access Channel information to the access terminals.").

248. *See id.*, § 8.3.6.2.6, p. 8-31 (Listing the following data fields for the AccessParameters message: MessageID, AccessCycleDuration, AccessSignature, OpenLoopAdjust, ProbeInitialAdjust, ProbeNumStep, PowerStep, PreambleLength, CapsuleLengthMax, Apersistence, and a Reserved field.).

249. *See*, *e.g.*, *id.*, § 8.3.6.1.4.1.1, p. 8-25 (using the OpenLoopAdjust and ProbeInitialAdjust data fields of the AccessParameters message for Access Probe power control).

250. *See*, *e.g.*, *id.*, § 8.3.6.1.4.1.1, p. 8-25 (using the SectorID and ColorCode data fields of the Overhead Messages for Access Channel long code mask).

251. During Access Attempts, in addition to configuring transmissions using data fields contained in the AccessParameters message and Overhead Messages, the Access Terminal also uses various well known fall-back data values or data values as designated by the Access Network via ConfigurationRequest messages (sent according to the the Generic Configuration Protocol) containing complex attributes including the InitialConfiguration Attribute and the PowerParameters Attribute (both of which contain numerous data fields and records sent to and stored by the Access Terminal). *See id.*, § 8.3.7, p. 8.36-8.38.

iii. Establishing an open session with the Access Network.

As noted in Section III(B)(3)(c)(ii), *supra*, the access channel physical layer packets initially sent by the Access Terminal during the Access Probe process contain data used to establish a session. Prior to establishing a session, "there are no communications between the access terminal and the access network."[252] The Access Network "may be unaware of the access terminal's existence within its coverage area."[253] "Other than to open a session, an access terminal cannot communicate with an access network without having an open session."[254] "An HRPD session refers to a shared state between the access terminal and the access network. This shared state stores the protocols and protocol configurations that were negotiated and are used for communications between the access terminal and the access network."[255] A session should not be confused with a connection.[256] In order to communicate with the Access Network over the air interface, the Access Terminal opens a session. In order to communicate with the Internet, the Access Terminal uses the established session to open a connection with the underlying Packet Data Serving Node linked to the

252. *Id.*, § 5.3.7.1.4, p. 5.23.

253. *Id*.

254. *Id.*, § 1.9, p. 1.12.

255. ANSI/TIA-878-2, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 1.4.2, p. 1.4.

256. *See id.* ("An air interface connection is a particular state of the air-link in which the access terminal is assigned a Forward Traffic Channel, a Reverse Traffic Channel and associated Medium Access Control (MAC) Channels.").

Access Network.[257] "During a single session the access terminal and the access network can open and close a connection multiple times[.]"[258] For session establishment, a powered-on Access Terminal will automatically initiate a session with a trusted Access Network without intervention or action from the user of the device.[259]

The first step to establishing a session where no prior session exists is for the Access Terminal to enter the Setup State[260] of the Default Address Management Protocol.[261] Once in the Setup State, the Access Terminal requests a Unicast Access Terminal Identifier (UATI) using the UATIRequest message.[262] For the Access Network, the UATI allows for "distinguishing among the different packets and [for] finding out which packet is from which

257. *See Technical Explanations*, Section III(B)(3)(c)(vi), *infra* (explaining the 1xEV-DO Rel. 0 connection establishment process).

258. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 5.11, p. 5.1.

259. The automatic nature of session establishment is unlike connection establishment which requires direct action by the Access Terminal user. *See Technical Explanations*, Section III(B)(3)(c)(vi), *infra* (explaining the 1xEV-DO Rel. 0 connection establishment process).

260. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 5.3.7.1.5, p. 5.24 ("In this state, the access terminal sends a request to the access network asking for a UATI and waits for the access network's response.").

261. *See id.*, § 5.3.1, p. 5.17 ("The Default Address Management Protocol provides the following functions: [] Initial UATI assignment[, and] Maintaining the access terminal unicast address as the access terminal moves between subnets.").

262. *See id.*, § 5.3.7.1.5.1, p. 5.24 ("Upon entering the Setup State the access terminal shall... send a UATIRequest message."); 5.3.7.2.1, p. 5.28 ("The access terminal sends the UATIRequest message to request that a UATI be assigned or re-assigned to it by the access network.").

AT."[263] More precisely, the UATI is a unique 32-bit numerical address[264] used by the Access Terminal and Access Network MAC layer protocols to label and identify transmissions during the current session.[265][266] When the Access Network receives the UATIRequest message, it transmits a UATIAssignment message that assigns a UATI to the Access Terminal for the session.[267] The UATIAssignment message is a unicast transmission containing numerous data fields that are written to the Access Terminal's internal storage.[268] The Access Terminal uses

263. Yang, *3G CDMA2000: Wireless System Engineering*, p. 229 ("[W]hen an AN receives an access channel MAC packet, it checks the *access terminal identifier record* field of the MAC layer header and performs address matching").

264. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 10.2, p. 10.2 ("The Access Terminal Identifier record provides a unicast, multicast, or broadcast access terminal address.").

265. *See*, *e.g.*, *id.*, § 8.2.6.1.4.2.4, p. 8.13 (Under a heading titled "Address Matching" applicable to transmission received from the Forward Control Channel, the standard explains that the "Access terminal shall forward the Security Layer packet along with the SecurityLayerFormat and the ConnectionLayerFormat fields to the Security Layer if... the ATIType field and the ATI field of the ATI Record in the MAC Layer header of a Security Layer packet is equal to the ATIType and ATI fields of any member of the Address Management Protocol's ReceiveATIList."); *id.*, 8.2.6.2.1, p. 8.14 (All MAC Layer Headers placed in front of Access Network transmitted Security Layer packets must contain the Access Terminal's "ATI Record.").

266. The UATI is also sent by the Access Terminal to the new Access Network (target) during a Connected State Route Update so that "the source AN [][can lookup] the session configuration parameters that are requested by the target[]" over the A13 interface. ANSI/TIA-878-2, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 2.4, p. 2.3; *see also Technical Explanations*, Section III(B)(3)(d) *et seq.*, *infra* (explaining Route Updates, *i.e.*, handoffs).

267. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 5.3.7.1.5.2, p. 5.24-5.25.

268. *See id.*, § 5.3.7.2.2, p. 5.29 (Listing the following data fields for the UATIAssignment message: MessageID, MessageSequence, Reserved1, SubnetIncluded, UATISubnetMask,

the data transmitted via the UATIAssignment message, to deduce its assigned 32-bit UATI[269] [270] and adds the UATI to its internally stored ReceiveATIList.[271] Once the Access Terminal adds its assigned UATI to its ReceiveATIList, it stops using the Default Address Management Protocol and begins using the Default Session Configuration Protocol. This second protocol is used to negotiate and configure a set of additional protocols to be used during the session.[272] For example, the Default Session Configuration Protocol is used to negotiate and configure the Security Layer protocols discussed in Section III(B)(3)(c)(iv), *infra*. Once all relevant protocols are negotiated and configured, the session is open and "the access terminal and the access network use the negotiated protocols to exchange data and signaling in accordance with the requirements of each protocol."[273] In other words, once a session is established, the Access Terminal can initiate a connection with the Access Network for the ultimate purpose of gaining access to the Internet. *See Technical Explanations*, Section III(B)(3)(c)(vi), *infra* (explaining the connection establishment process).

UATI104, UATIColorCode, UATI024, UpperOldUATILength, and a Reserved2 field).

269. *See id.*, § 5.3.7.1.5.1, p. 5.24-5.25.

270. The UATI is unrelated to the Access Terminal's internally stored ESN.

271. *See id*.

272. *See id.*, § 5.4.1, p. 5.35 ("The Default Session Configuration Protocol provides for the negotiation and configuration of the set of protocols used during a session.").

273. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 5.4.6.1.6, p. 5.44.

iv. Application of encryption and authentication keys for use in the security layer.

During session establishment, the Access Terminal and Access Network negotiate and configure the security layer protocols so that a session key may be created for use in data integrity, authentication, and encryption in the MAC layer. The session key is created using a session key exchange process, which "[p]rovides the procedures followed by the access network and by the access terminal to exchange security keys for authentication and encryption."[274] The authentication keys are used "by the access network and the access terminal for authenticating traffic [(*i.e.*, data)]."[275] Traffic authentication is done through a cryptographic authentication process[276] allowing for the Access Network and Access Terminal to ensure that transmissions being received are not coming from a man-in-the-middle who may be altering data or impersonating either the Access Network or Access Terminal.[277]

274. *Id.*, § 7.1.1, p. 7.1.

275. *Id.*

276. "Authentication is a service that is used to establish the origin of information. That is, authentication services verify the identity of the user or system that created information (*e.g.*, a transaction or message). This service supports the receiver in security relevant decisions, such as 'Is the sender an authorized user of this system?' or 'Is the sender permitted to read sensitive information?' Several cryptographic mechanisms may be used to provide authentication services...." National Institute of Standards and Technology, NIST Special Publication 800-57, *Recommendations for Key Management -- Part 1: General (Revised)* (Mar. 2007), p. 30.

277. The type of man-in-the-middle attack protection provided in the 1xEV-DO Rel. 0 security layer is limited to scenarios where the attacker attempts to mimic a party *after* session establishment. Other types of 1xEV-DO Rel. 0 man-in-the-middle attacks, such as those launched *prior* to session establishment, are not prevented by the MAC payload authentication provided in the security layer. As explained later in this subsection, the various authentication keys are ultimately derived from Hash-based Key Derivation Function using a shared secret (*i.e.*, the the session key or "SKey") created through the Diffie-Hellman Pair-Wise Key Establishment Scheme. "The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. In this attack, an opponent Carol intercepts Alice's public value and sends her

The encryption keys are used "by the access network and the access terminal for encrypting traffic [(*i.e.*, data)]."[278] Traffic encryption is done through a cryptographic encryption process[279] allowing for the Access Network and Access Terminal to exchange data that cannot be read by third-party eavesdroppers even if they gain full access to all transmissions. The noted encryption keys are used to encrypt all data content and signaling information in the MAC layer payload, which contains all higher layer protocol data units.[280] In other words, if encryption is invoked by the Access Network, all forward and reverse link

own public value to Bob. When Bob transmits his public value, Carol substitutes it with her own and sends it to Alice. Carol and Alice thus agree on one shared key and Carol and Bob agree on another shared key. After this exchange, Carol simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants." RSA Laboratories [website], *RSA Laboratories - 3.6.1 What is Diffie-Hellman?*, http://www.rsa.com/rsalabs/node.asp?id=2248 (last accessed: Mar. 23, 2012). Applying the above scenario to 1xEV-DO Rel. 0 with its use of Diffie-Hellman without supplementary two-party authentication, Carol operates a cell site emulator to become a man-in-the-middle between Bob's Access Terminal and Alice's legitimate wireless carrier cell site.

278. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 7.1.1, p. 7.1.

279. "Encryption is used to provide confidentiality for data. The data to be protected is called plaintext when in its original form. Encryption transforms the data into ciphertext. Ciphertext can be transformed back into plaintext using decryption. The Approved algorithms for encryption/decryption are symmetric key algorithms: AES and TDEA...." NIST Special Publication 800-57, *Recommendations for Key Management -- Part 1: General (Revised)*, p. 35.

280. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 8.1.2, p. 8.2-8.4, Fig. 8.1.2-1 ("Control Channel MAC Layer Packet Encapsulation"), Fig. 8.1.2-2 ("Access Channel MAC Layer Packet Encapsulation"), Fig. 8.1.2-3 ("Forward Traffic Channel MAC Layer Packet Encapsulation"), and Fig. 8.1.2-4 ("Reverse Traffic Channel MAC Layer Packet Encapsulation").

data content and signaling information are protected from eavesdroppers over the air interface.[281]

During the session key exchange process, the Access Network and Access Terminal use the DH Key Exchange Protocol outlining "a method for session key exchange based on Diffie-Hellman (DH)."[282] "The Diffie-Hellman (DH) key exchange protocol provides a method for session key exchanges based on the DH key exchange algorithm."[283] The Diffie-Hellman key exchange algorithm is an asymmetric key algorithm[284] allowing for "two users to exchange a secret key over an insecure medium without any prior secrets."[285] In Diffie-Hellman, "both parties contribute information to the key agreement process."[286] The Diffie-Hellman session

281. Although the MAC layer payload is encrypted, the MAC layer header, which is neither encrypted nor authenticated, contains the Access Terminal Identifier (*e.g.*, the UATI) in plaintext. *See id.*, § 8.6.2.1, p. 8.14. However, as explained in the *Technical Explanations*, Section III(B)(3)(c)(iii), *supra*, the UATI is a randomly assigned value used for MAC layer addressing purposes and it cannot be used by an eavesdropper to identify Access Terminal hardware.

282. *Id.*, § 7.6.1., p. 7.22.

283. Rhee, Man Y., *Mobile Communication Systems and Security*, John Wiley & Sons (Jin Xing Distripark, Singapore: 2009), p. 222.

284. "Asymmetric key algorithms, commonly known as public key algorithms, use two related keys (*i.e.*, a key pair) to perform their functions: a public key and a private key. The public key may be known by anyone; the private key **should** be under the sole control of the entity that "owns" the key pair. Even though the public and private keys of a key pair are related, knowledge of the public key does not reveal the private key." NIST Special Publication 800-57, *Recommendations for Key Management -- Part 1: General (Revised)*, p. 35 (footnote omitted).

285. RSA Laboratories [website], *RSA Laboratories - 3.6.1 What is Diffie-Hellman?*, http://www.rsa.com/rsalabs/node.asp?id=2248 (last accessed: Mar. 23, 2012).

286. National Institute of Standards and Technology, NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key*

key created by the Access Network and Access Terminal is referred to as the SKey and is either a 768-bit key or 1024-bit key.[287] After the Skey is created, the Access Network and Access Terminal separately split their SKey copies into "eight sub-fields within the SKey. These sub-fields are of equal length."[288] The eight sub-fields are then used with Hash-based Key Derivation Functions (HKDFs)[289] to create four pairs of 160-bit authentication and encryption key values for use on each of the forward and reverse link channels transmitted/received by the Access Network and Access Terminal.[290] Each of the four 160-bit authentication keys are used to authenticate packets on their respective channels[291] via Keyed-Hash Message

Lengths (Jan. 2011), p. 7.

287. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 7.6.7, p. 7.48, Tab. 7.6.7-1.

288. *Id.*, § 7.6.5.1.3, p. 7.28.

289. "Cryptographic hash functions can be used as building blocks in key derivation functions (KDFs).... KDFs using cryptographic hash functions as their building blocks are called Hash-based Key Derivation Functions (HKDFs). The main purpose of an HKDF is to generate (*i.e.*, derive) secret keys from a secret value (*e.g.*, a shared key, or a shared secret in a key agreement scheme) that is shared between communicating parties. The security strengths of the derived secret keys are limited to the security strength of the secret value. The security strength of the secret value shall meet or exceed the desired security strengths of the derived secret keys." National Institute of Standards and Technology, NIST Special Publication 800-107, *Recommendation for Applications Using Approved Hash Algorithms* (Feb. 2009), p. 14.

290. *Id.*, § 7.6.5.1.3, p. 7.28-7.29 and Fig. 7.6.5.1-1 ("Message Bits for Generation of Authentication and Encryption Keys").

291. IS-856 only defines procedures "for authentication of access channel MAC layer packets by applying the SHA-1 hash function to message bits (ACPAC - Access Channel MAC Layer Packet Authentication Code)." Korowajczuk, *Designing cdma2000 Systems*, p. 338. However, data integrity and authentication of packets sent over traffic channels and the control channel can also be implemented by any 1xEV-DO Rel. 0 network considering authentication keys are defined and generated for "the Forward Traffic Channel" (*i.e.*, FACAuthKey), "the Reverse Traffic Channel" (*i.e.*, RACAuthKey), and "the Control Channel" (*i.e.*, FPCAuthKey).

Authentication Codes (HMACs)[292] derived from the SHA-1 cryptographic hash function.[293] For encryption purposes, each of the four 160-bit encryption keys are truncated into 128-bit AES (based on Rijndael)[294] encryption keys which are used for encrypting packets on their respective channels[295] via the AES symmetrical key algorithm.[296]

TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 7.6.3.2, p. 7.22.

292. "Message authentication codes (MACs) provide data authentication and integrity protection.... MAC algorithms that are based on cryptographic hash functions[] [are] called HMAC algorithms... The HMAC output is generated from the secret key and the string of 'text' to be MACed (*e.g.*, a message to be sent) using the HMAC algorithm. The MacTag is provided to the MacTag verifier, along with the 'text' that was MACed (*e.g.*, the sender transmits both the MacTag and the 'text' that was MACed to the intended receiver). [] The verifier computes an HMAC output on the received 'text' using the same key and HMAC algorithm that was used by the HMAC generator, generates a MacTag (either a full or truncated HMAC output), and then compares the generated MacTag with the received MacTag. If the two values match, the 'text' has been correctly received, and the verifier is assured that the entity that generated the MacTag is a member of the community of users that share the key." NIST Special Publication 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, p. 12.

293. SHA-1, as well as SHA-224, SHA-256, SHA-384, SHA512, SHA-512/224 and SHA-512/256, are all "iterative, one-way hash functions that can process a message to produce a condensed representation called a message digest. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and message authentication codes, and in the generation of random numbers or bits." National Institute of Standards and Technology, FIPS PUB 180-4, *Federal Information Processing Standards Publication: Secure Hash Standard (SHS)* (Mar. 2012), p. 3.

294. AES, based on Rijndael, is "a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in [][the AES] standard." National Institute of Standards and Technology, FIPS PUB 197, *Announcing the Advanced Encryption Standard (AES)* (Nov. 26, 2001), p. 5.

295. *See* Telecommunications Industry Association, TIA-925-1 [E] (Addendum to TIA-925),

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

If attempting to crack 1xEV-DO Rel. 0 security layer encryption via cryptanalysis,[297] the 1024-bit Diffie-Hellman asymmetrical keys and the 128-bit AES symmetrical keys are considered secure for the year 2008.[298] In general terms, the protections provided by encryption are primarily based on current computer technology being unable to quickly compute values using factoring algorithms and discrete logarithm attacks. "The first successful factorization of a 768-bit RSA modulus was not reported until December 2009. This effort required six months of computations using highly sophisticated equipment. According to the paper's authors, factoring a 1024-bit modulus would be 'one thousand times harder' than a 768-bit one. This means that another 6-7 years are likely to pass before 1024-bit numbers could

Enhanced Subscriber Privacy for cdma2000 High Rate Packet Data - Addendum 1 (Arlington, VA: Sept. 2007), § 3, p. 3-1 ("The AES Encryption Protocol uses the AES (a.k.a. Rijndael) procedures defined in [][3GPP2 S.S0055-A] in order to encrypt the Connection Layer packets and decrypt the Authentication Protocol packets."); § 3.5.1.1, p. 3.3-3.6 ("Constructing the Encryption Key").

296. "Symmetric key algorithms (sometimes known as secret key algorithms) transform data in a way that is fundamentally difficult to undo without knowledge of a secret key. The key is "symmetric" because one key is used for all operations (*e.g.*, encryption and decryption). Symmetric keys are often known by more than one entity; however, the key shall not be disclosed to entities that are not authorized access to the data protected by that algorithm and key." NIST Special Publication 800-57, *Recommendations for Key Management -- Part 1: General (Revised)*, p. 34.

297. Cryptanalysis: "Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection." *Id.*, p. 20.

298. *See* NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths* (Jan. 2011), p. 3-4, "Table 1: Encryption Transitions" (listing use of AES 128-bit encryption keys as "Acceptable"); *id.*, p. 7-8, "Table 4: SP 800-56A Key Agreement (DH and MQV)" (listing use of Diffie-Hellman 1024-bit encryption keys as "Acceptable through 2010[;] Deprecated from 2011 through 2013[;] Disallowed after 2013").

realistically be factored."[299] The 768-bit number factored in December of 2009 was in the context of RSA—an asymmetrical cryptographic algorithm using integer factorization cryptography as apposed to the discrete logarithm cryptography used in Diffie-Hellman.[300] However, NIST issues the same key length "comparable strengths" recommendations for Diffie-Hellman as it does for RSA[301] and the required computational requirements for cryptanalysis under each cryptographic scheme are similar.[302] Therefore, 1024-bit encryption keys in the context of Diffie-Hellman will be uncrackable at least until the year 2017. In comparison to Diffie-Hellman, the 128-bit AES keys used in 1xEV-DO Rel. 0 offer an even less likely entry point for an attacker. Seagate Technology, LLC took a simplistic approach to a difficult cryptanalysis question and determined that it would take 70 billion computers 77,000,000,000,000,000,000,000,000 (77 trillion trillion) years to crack one 128-bit AES encryption key using computer technology and cryptanalysis techniques available in the year

299. NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Appendix A: Decision Rationale, § A.2.

300. *Compare* NIST Special Publication 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography* (Aug. 2009) *with* NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)* (Mar. 2007).

301. *See* NIST Special Publication 800-57, *Recommendations for Key Management -- Part 1: General (Revised)*, p. 63, "Table 2: Comparable strengths."

302. Pornin, Thomas, "How to calculate the time it'll take to crack RSA or DH?," online posting, Oct. 6, 2011, *diffie hellman - How to calculate the time it'll take to crack RSA or DH? - Cryptography - Stack Exchange*, http://crypto.stackexchange.com/questions/913/how-to-calculate-the-time-itll-take-to-crack-rsa-or-dh (last accessed: Apr. 9, 2012) (explaining how cracking discrete logarithm cryptographic keys has the same, or slightly greater, asymptotic complexity as cracking integer factorization cryptographic keys).

2008.[303]

Regardless of available key strengths, 1xEV-DO Rel. 0 encryption will only protect data if it is implemented by the Access Network. At the beginning of session establishment and prior to the session key exchange process, the Access Network and Access Terminal use the Default Encryption Protocol, which provides no encryption for signals transmitted over the air interface.[304][305] The Access Network and Access Terminal will continue to use the Default Encryption Protocol until the Access Network initiates the session key exchange process.[306] [307] However, initiation of the session key exchange process is not required[308][309] and the

303. Seagate [technical paper], *128-Bit Versus 256-Bit AES Encryption: Practical business reasons why 128-bit solutions provide comprehensive security for every need*, p. 4, *available at* http://www.seagate.com/staticfiles/docs/pdf/whitepaper/tp596_128-bit_versus_256_bit.pdf (last accessed: Apr. 9, 2012).

304. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 7.9, p. 7.68 ("The Default Encryption Protocol does not alter the Security Layer packet payload (i.e., no encryption/decryption) and does not add an Encryption Protocol Header or Trailer; therefore, the Cipher-text for this protocol is equal to the Connection Layer packet.").

305. Likewise, the "Default Authentication Protocol does not provide any services except for transferring packets between the Encryption Protocol and the Security Protocol." *Id.*, § 7.7.1, p. 7-56.

306. *See id.*, § 7.6.5.1.2, p. 7.26 ("The access network shall initiate the key exchange by sending a KeyRequest message.").

307. If following good security practices, a wireless carrier Access Network will initiate the session key exchange process (in order to "turn on" encryption and authentication) as soon as possible, *i.e.*, after the UATI is assigned to the Access Terminal.

308. *See* Korowajczuk, *Designing cdma2000 Systems*, p. 359 ("[E]ven though a single layer may contain multiple protocols, each of them can be individually negotiated to better accommodate network requirements and availability.").

309. There is no logical reason why a wireless carrier would not implement the encryption procedures provided via the security layer.

Default Encryption Protocol can be used during the entire session if the Access Network chooses to not use encryption. If the Access Network chooses to not initiate the session key exchange, all communications content and signaling information contained in the MAC payload will not be encrypted via the security layer.[310] If security layer encryption is not used, "end-to-end encryption can be provided at the application layer"[311] to protect communications content contained in higher layer protocol data units sent over Traffic Channels. However, the security layer encryption explained in this section is still the only mechanism that will protect Access Channel and Control Channel signaling information from being intercepted over the air interface. An Access Network's failure to initiate the session key exchange process will result in signaling information, such as the Access Terminal's ESN transmitted in response to a HardwareIDRequest message, being exposed to third-party eavesdroppers.

v. Obtaining identifying information from Access Terminal hardware using the HardwareIDRequest message.

Once a session is established, the Access Network can obtain the Access Terminal's identifying information by transmitting a HardwareIDRequest message.[312] By transmitting a HardwareIDRequest message, the Access Network asks the Access Terminal to transmit a HardwareIDResponse message[313] containing its ESN or other "unique ID that has been

310. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 7.9, p. 7.68.

311. *Id*.

312. *See id.*, § 5.3.7.1.3, p. 5.23; *see also id.*, § 5.3.7.2.4, p. 5.31.

313. *See id.*, § 5.3.7.2.5, p. 5.31 ("The access terminal sends this message in response to the HardwareIDRequest message.").

assigned to the terminal by the manufacturer."[314] Prior to receiving the HardwareIDResponse message, the Access Network identifies the Access Terminal generically via reverse link PN codes and the Access Terminal's UATI assigned by the Access Network.[315] The Access Terminal's HardwareIDResponse message provides its absolute identity, which can be used to determine the customer who's wireless account is associated with the Access Terminal. Although not precisely articulated in the relevant standards, the main purpose served by the HardwareIDRequest message is to provide the Access Network with an initial Access Terminal identity verification mechanism.[316] If the ESN or MEID contained in the HardwareIDResponse message does not belong to a device authorized for service then the wireless carrier can direct the Access Terminal away from the Access Network prior to any attempt to open a connection. By severing the air link with the unauthorized Access Terminal during the session but prior to establishing a connection, network resources are conserved.

vi. Opening a connection with the Access Network.

Once a session is established, the user of the Access Terminal can initiate the connection process with the Access Network. In the case of an aircard, the connection process is initiated

314. *Id*.

315. *See Technical Explanations*, Section III(B)(3)(c)(iii), *supra* (UATI used to identify the Access Terminal).

316. *See*, *e.g.*, Nortel Networks, PN-4875/IS-856 Ballot Comments, *AT Authentication in 1xEV-DO*, p. 1 ("In this comment, AT hardware authentication is added as a part of the Address Management Protocol (ADMP) in the Session Layer. This allows an operator to perform terminal authentication, based on a hardware identifier (such as the IMSI) over the common channels before the AT is assigned a traffic channel.").

via software installed on the host laptop computer paired with the aircard.[317] For example, an aircard user may initiate the connection process by clicking a "connect" button on companion software bundled with the aircard. Once the user has initiated the connection process, the Access Terminal transitions into the Connection Setup Substate of the Idle State. In this substate, "the access terminal and the access network setup a connection[]"[318] via the previously explained Access Attempt process. Using Access Probes, "[t]he access terminal sends the ConnectionRequest message to request a connection."[319] Once the ConnectionRequest message is sent, indicating that the Access Terminal "is ready to exchange data on the access stream, the AN shall initiate PPP procedures..."[320] PPP is an acronym for "Point-to-Point Protocol" and provides a standard method for the Access Network and Access terminal to communicate.[321] "PPP also defines an extensible Link Control Protocol, which allows negotiation of an Authentication Protocol for authenticating its peer before allowing

317. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (government web research on UTStarcom PC5740 aircard indicating that it is bundled with "VZAccess Manager software for easy connection management.").

318. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.4.1, p. 6.26.

319. *Id.*, § 6.4.6.2.2, p. 6.39.

320. ANSI/TIA-878-2 (Addenda to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 2.3.1.1, p. 2.2.

321. *See* RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)* (Aug. 1996), p. i.

Network Layer protocols to transmit over the link."[322] In basic terms, PPP, as used in the Connection Setup Substate, allows the Access Network to positively authenticate the Access Terminal and determine if it is authorized to access 1xEV-DO Rel. 0 service.[323] In order to accomplish this task, 1xEV-DO Rel. 0 employs the Challenge-Handshake Authentication Protocol (CHAP)—an element of PPP.[324] CHAP is "used to periodically verify the identity of the peer using a 3-way handshake."[325] In 1xEV-DO Rel. 0, the peer is the Access Terminal and the Access Network is the authenticator ensuring that the peer is authorized to access the cellular data network.[326] CHAP depends on the peer (*i.e.*, the Access Terminal) and the authenticator (*i.e.*, the Access Network) having a previously shared secret that is not transmitted or exchanged during the CHAP process.[327] In 1xEV-DO Rel. 0, the shared secret is the Shared Secret Data (SSD)[328] stored within the Access Terminal's internal storage device

322. *Id*.

323. It was previously explained how the Access Network can *identify* an Access Terminal by obtaining its stored ESN via a HardwareIDRequest message. *See Technical Explanations*, Section III(B)(3)(c)(v), *supra*. However, obtaining an Access Terminal's ESN is only a preliminary identification mechanism and it is not sufficient for *authenticating* an Access Terminal for receiving service. Because an ESN can be copied by an attacker who has physical access to the Access Terminal, a more secure authentication mechanism using Shared Secret Data (SSD) (*i.e.*, PPP as explained in this subsection) is employed to positively authenticate the Access Terminal prior to receiving service.

324. *See* RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, p. 2.

325. *Id*.

326. Although CHAP can also be used by the Access Terminal to authenticate the Access Network, this is not done in 1xEV-DO Rel. 0.

327. *See id.*, p. 3 ("This authentication method depends upon a 'secret' known only to the authenticator and that peer. The secret is not sent over the link.")

328. "Shared Secret Data (SSD) is a 128-bit pattern stored in the MS and readily available to

(NAM)[329] with an exact copy stored in a database maintained by the Access Terminal's home "Access Network-Authentication, Authorization, and Accounting" (AN-AAA) server within the wireless carrier network.[330]

Once a PPP connection is established between the Access Network and Access Terminal, "[t]he AN generates a random challenge and sends it to the AT in a CHAP Challenge message..."[331] Once the Access Terminal receives the CHAP challenge, it concatenates some of the data contained in the challenge with its stored Shared Secret Data and then uses a cryptographic hashing algorithm to create a message digest[332] (*i.e.*, a "one-way hash") of the

---

the network. This Shared Secret Data is not passed across the air interface between the MS and the network..." Telecommunications Industry Association, TIA/EIA/IS-2001-A (Revision of TIA/EIA/IS-2001), *Interoperability Specifications (IOS) for cdma2000 Access Network Interfaces* (Arlington, VA: Aug. 2001), § 4.2.1, p. 290.

329. *See* TIA-683-D (Revision to TIA-683-C), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, § 3.5.8, p. 3.141, Table 3.5.8-1 3GPD Parameter Block Types (listing "HRPD Access Authentication CHAP SS Parameters" for the Access Terminal NAM (footnote omitted)); *id.*, § 3.5.8.14, p. 3.158 (showing the "SS" field of the "HRPD Access Authentication CHAP SS Parameters" as containing "Shared Secret Data").

330. *See* fn. No. 328, *supra*.

331. ANSI/TIA-878-2 (Addenda to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 3.1.1(d), p. 3.2.

332. Cryptographic hashing algorithms and message digests are generally explained in footnotes contained in the *Technical Explanations*, Section III(B)(3)(c)(iv), *supra* (MAC payload encryption and authentication in the security layer). However, use of a hashing algorithm for authentication and integrity checks of MAC layer payloads (as explained in the *Technical Explanations*, Section III(B)(3)(c)(iv), *supra*) is different from the authentication explained in this section. Previously, it was explained how a hashing algorithm is applied to message bits contained in MAC layer payloads. In this section, a hashing algorithm is employed so that the Access Network will be able to authenticate (*i.e.*, identify and authorize) the Access Terminal prior to providing it service.

result.[333] The resulting message digest is used in the CHAP challenge response message.[334] The "one-way hash" is essentially a unique signature taken of the concatenated data used to create the CHAP response. The Access Terminal then transmits its CHAP response message to the Access Network containing the calculated "one-way hash."[335] When the Access Network receives the CHAP response message, it forwards it to the AN-AAA server connected directly to the Access Network using an Access-Request message over the A12 interface.[336] If the AN-AAA server is not the Access Terminal's home AN-AAA, it will be unable to verify the CHAP response because it will not have a stored copy of the Access Terminal's Shared Secret Data. In this case, the visited AN-AAA forwards the CHAP response to the home network AN-AAA.[337] Once the appropriate AN-AAA receives the Access-Request message, it retrieves the Access Terminal's Shared Secret Data from its database and concatenates it with some of the data contained in the Access-Request message to create a "one-way hash" in the same fashion

333. *See* RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, p. 8 ("The Response Value is the one-way hash calculated over a stream of octets consisting of the Identifier, followed by (concatenated with) the 'secret', followed by (concatenated with) the Challenge Value.").

334. *See id*.

335. *See id.*, p. 7 ("Whenever a Challenge packet is received, the peer MUST transmit a CHAP packet with the Code field set to 2 (Response).").

336. *See* ANSI/TIA-878-2 (Addenda to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 3.1.1(e), p. 3.2.

337. *See id.*, § 2.3.3, p. 2.3 ("If the AN-AAA does not have the authority to accept/deny the request, it forwards the request to the home network...").

explained for the Access Terminal.[338] If the "one-way hash" created by the AN-AAA matches the "one-way hash" contained in the CHAP response message (created by the Access Terminal), the AN-AAA sends the Access Network an Access-Accept message.[339] Otherwise, the AN-AAA sends the access Network an Access-Reject message indicating that the Access Terminal is not authorized for 1xEV-DO Rel. 0 service.[340]

In the case of an Access-Reject message, "[t]he AN returns an indication of CHAP access authentication failure to the AT[]"[341] and "sends a SessionClose message to the AT to close the HRPD session."[342] In the case of an Access-Accept message, "[t]he AN returns an indication of CHAP access authentication success to the AT[]"[343] and then begins other steps to register the Access Terminal on the network so that Internet access service can be provided by the Packet Data Serving Node (PDSN). In order to register the Access Terminal for Internet access, the Access Network establishes a connection with the Packet Control Function (PCF).[344] The Packet Control Function then "sends an A11-Registration Request message to the

338. *See* RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*, p. 7 ("Whenever a Response packet is received, the authenticator compares the Response Value with its own calculation of the expected value.")

339. *See* ANSI/TIA-878-2 (Addenda to TIA-878), *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 3.1.1(f), p. 3.2.

340. *See id.*, § 3.1.2(f), p. 3.3.

341. *Id.*, § 3.1.2(g), p. 3.3.

342. *Id.*, § 3.1.2(h), p. 3.3.

343. *Id.*, § 3.1.1(g), p. 3.2.

344. *See id.*, § 3.1.1(j), p. 3.2.

PDSN..."[345] "The A11-Registration Request message is validated and the PDSN accepts the connection by returning an A11-Registration Reply message with an accept indication..."[346] [347] Once the Packet Data Serving Node accepts the connection through the registration process, the Packet Control Function notifies the Access Network,[348] a "PPP connection establishment procedure is performed between the AT and the PDSN...,"[349] and "the connection is established and packet data [(*i.e.*, Internet traffic)] can flow between the AT and the PDSN."[350] Once the connection is established, the Access Terminal transitions from the Idle State to the Connected State.[351]

345. *Id.*, § 3.1.1(k), p. 3.2.

346. *Id.*, § 3.1.1(l), p. 3.2.

347. In other words, the "registration" process in 1xEV-DO Rel. 0 occurs between the PCF and PDSN—not between the Access Terminal and Access Network. *See also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 055 of *2nd Consolidated Exhibits* (Dkt. #821-3) (diagram from ANSI/TIA-878-2 (Addenda to TIA-878) showing 1xEV-DO registration process occurring between PCF and PDSN over the A11 interface, *i.e.*, not between the Access Terminal and Access Network).

348. *See id.*, § 3.1.1(m), p. 3.2.

349. *Id.*, § 3.1.1(n), p. 3.2.

350. *Id.*, § 3.1.1(o), p. 3.2.

351. Other than power control and route updates, the numerous complex operations applicable to the 1xEV-DO Rel. 0 Connected State are beyond the scope of the aircard locating mission in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.) and are therefore not discussed in the *Technical Explanations*.

d. Using the Default Route Update Protocol to scan for additional pilots, facilitate sector Route Updates, and send Route Update messages.

In addition to searching for pilots during the Pilot Acquisition Substate,[352] the Access Terminal also searches for pilots to facilitate use of the Default Route Update Protocol. "The Default Route Update Protocol provides the procedures and messages used by the access terminal and the access network to keep track of the access terminal's approximate location and to maintain the radio link as the access terminal moves between the coverage areas of different sectors."[353] In order to serve the goals of the Default Route Update Protocol, "[t]he access terminal shall continually search for pilots in the Connected State and whenever it is monitoring the Control Channel in the Idle State."[354] During the searching process, "[t]he access terminal estimates the strength of the Forward Channel transmitted by each sector in its neighborhood."[355] "The access terminal shall measure the strength of every pilot it searches."[356] When the Access Terminal finds additional pilots transmitting in its neighborhood, it stores the pilots in sets according to signal strength.[357] In addition to searching for pilots in its neighborhood, the Access Terminal "should also be capable of

352. *See Technical Explanations*, Section III(B)(3)(b)(ii), *supra*.

353. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.6.1, p. 6.55.

354. *Id.*, § 6.6.6.1.2.2, p. 6.64.

355. *Id.*, § 6.6.6.1.2, p. 6.62.

356. *Id.*, § 6.6.6.1.2.3, p. 6.64.

357. *See id.*, § 6.6.6.1.2, p. 6.62.

searching for pilots in frequencies and band classes other than its current frequency."[358] In order to locate the maximum amount of available Access Networks, the Access Terminal will search all listed frequencies in its Preferred Roaming List Acquisition Table for additional pilots and it may also receive additional frequencies to search via channel records provided by the Access Network in real-time.[359] If a transmitted pilot "is on a different frequency assignment from that of the mobile station, this target frequency should be included in the search criteria."[360]

The Access Terminal maintains the following continuously updated sets of searched pilots: (1) Active Set, (2) Candidate Set, (3) Neighbor Set, and (4) Remaining Set.[361] The Active Set is "[t]he set of pilots [] associated with the sectors currently serving the access terminal."[362] "When a connection is open [(*i.e.*, in the Connected State)], a sector is considered to be serving an access terminal when there is a Forward Traffic Channel, Reverse Traffic Channel and Reverse Power Control Channel assigned to the access terminal. When a connection is not open [(*i.e.*, in the Idle State)], a sector is considered to be serving the access

358. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 154.

359. *See*, *e.g.*, TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.8.6.2.2, p. 6.125 (Indicating that the "NeighborChannel" parameter for the SectorParameters message consists of the "Channel record specification for the neighbor channel.").

360. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 154.

361. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.6.6.1.2, p. 6.62-6.63.

362. *Id*.

terminal when the access terminal is monitoring that sector's control channel."[363] The remaining three sets of pilots are categorized according to various rules and are maintained for conducting Route Updates where appropriate, *i.e.*, Access Terminal handoffs[364] from one Access Network to another.

i. Operations of the Default Route Update Protocol specific to the Idle State.

While in the Idle State, the Access Terminal maintains the Active Set of pilots on its own without receiving instructions from any Access Network.[365] "The access terminal shall initially keep an Active Set of size one when it is in the Idle State. The Active Set pilot shall be the pilot associated with the Control Channel the access terminal is currently monitoring."[366] The Access Terminal continuously compares the pilots maintained in the four pilot sets and

363. *Id*.

364. A handoff is "[t]he act of transferring communication with an access terminal from one sector to another." Telecommunications Industry Association, TIA-866-A (Revision of TIA-866), *Introduction to cdma2000 Spread Spectrum Systems* (Arlington, VA: Jan. 2006), § 1.2.1, p. 1.3. In 1xEV-DO, the term "route update" is typically used in place of "handoff." There are two primary types of handoffs in 1xEV-DO Rel. 0 that occur various states: the "hard handoff" and the "soft handoff." A hard handoff is "characterized by a temporary disconnection of the Traffic Channel. Hard handoffs occur when the access terminal changes to a new CDMA frequency." *Id.*, § 1.2.1, p. 1.5. In contrast, a soft handoff is "a handoff occurring while the access terminal is in the Connected State of the Default Route Update Protocol. This handoff is characterized by pointing the DRC from one sector to another on the same CDMA frequency assignment." *Id.*, § 1.2.1, p. 1.8.

365. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.6.1, p. 6.55 ("In [][the Idle] State, the access terminal autonomously maintains the Active Set.").

366. *Id.*, § 6.6.6.1.5.1, p. 6.69.

uses "pilot strengths to decide which sector's Control Channel it monitors."[367] For example, if the pilot of the Access Network acquired by the Access Terminal after initial power-on has a lower signal strength compared to a newly searched pilot then the Access Terminal will stop monitoring the first Access Network sector Control Channel and it will begin monitoring the new Access Network sector Control Channel.[368] This process is called an Idle State Route Update (*i.e.*, idle handoff)[369] and is initiated by the Access Terminal without direct involvement from any Access Network.[370]

Idle State Route Updates occur under two scenarios: (1) before session establishment, and (2) after session establishment but before connection establishment. An Access Terminal conducting an Idle State Route Update prior to session establishment can seamlessly switch to any Access network, even if part of a different system (*i.e.*, subnet), without having to send transmissions to any Access Network.[371] However, an Access Terminal conducting an Idle

367. *Id.*, § 6.6.6.1.2, p. 6.62.

368. While monitoring the Control Channel of the new Access Network, the Access Terminal receives and processes the new Access Network's Overhead Messages as explained in the *Technical Explanations*, Section III(B)(3)(c)(i), *supra*. As long as the new Access Network belongs to a preferred system, as listed on the Access Terminal's Preferred Roaming List System Table, the Idle State Route Update completes.

369. An idle handoff is "[t]he act of transferring reception of the Control Channel from one sector to another, when the access terminal is in the Idle State of the Default Route Update Protocol." TIA-866-A (Revision of TIA-866), *Introduction to cdma2000 Spread Spectrum Systems*, § 1.2.1, p. 1.5.

370. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 154 ("During this search, if the mobile station detects a pilot channel signal from another base station that is sufficiently stronger than that of the current base station, the mobile station determines that an idle handoff should occur.").

371. An Access Terminal can initiate an autonomous Idle State Route Update prior to session

State Route Update after session establishment, but before connection establishment, needs to either close the current session and open a new session with the new Access Network or the wireless carrier needs to use the A13 interface to transfer authentication and session configuration parameters similar to what is implemented for Connected State Route Updates.[372] While in the Idle State, if a session is established or is being established, the Access Terminal sends the Access Network "RouteUpdate messages to update its location with the access network."[373][374] The Access Terminal transmits RouteUpdate messages either when "the computed value *r* is greater than the value provided in the RouteUpdateRadius field of the SectorParameters message transmitted by the sector in which the access terminal last sent a RouteUpdate message[,]"[375] or "whenever it transmits on the Access Channel."[376]

---

establishment because the Default Session Management Protocol is in the Inactive State until the Access Probe process. "In this state there are no communications between the access terminal and the access network. The access terminal does not maintain any session-related state and the access network may be unaware of the access terminal's existence within its coverage area when the access terminal's Session Management Protocol is in this state." TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 5.2.6.1.4, p. 5.9.

372. *See Technical Explanations*, Section III(B)(3)(d)(ii), *infra*.

373. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 6.6.6.1.5.4, p. 6.70. In other words, while in the Idle State, "RouteUpdate messages from the access terminal are based on the distance between the sector where the access terminal last sent a RouteUpdate message and the sector currently in its active set." *Id.*, § 6.6.6.1.5, p. 6.69.

374. *See id.*, § 6.6.6.2.1, p. 6.76 (Listing the following data fields for the RouteUpdate message: MessageID, MessageSequence, ReferencePilotPN, ReferencePilotStrength, ReferenceKeep, NumPilots, PilotPNPhase, ChannelIncluded, Channel, PilotStrength, Keep, and a Reserved field.).

375. *Id.*, § 6.6.6.1.5.4, p. 6.71.

376. *Id.*, § 6.6.6.1.5.4, p. 6.70.

ii. Operations of the Default Route Update Protocol specific to the Connected State.

While in the Connected State, the Access Network dictates the Access Terminal's Active Set of pilots.[377] "The access network determines the contents of the Active Set through TrafficChannelAssignment messages."[378] These messages contain various data fields[379] including the pilots (labeled as PilotPN field) belonging to the Access Networks the Access Terminal must access for receiving Internet access service. "If the access terminal receives a valid TrafficChannelAssignment message, it shall replace the contents of its current Active Set with the pilots specified in the message."[380] In other words, while a connection is established, the Access Network dictates the list of additional Access Networks the Access Terminal must choose from when conducting Route Updates (*i.e.*, handoffs). While in the Connected State, and unlike in the Idle State, the Access Terminal sends "RouteUpdate message[s] to the access network... to request addition or deletion of pilots from its Active Set."[381] The Access Terminal transmits RouteUpdate messages when there are "changes in the radio link between the access terminal and the access network, obtained through pilot strength measurements at

377. *See id.*, § 6.6.1, p. 6.55 ("In [][the Connected] state the access network dictates the access terminal's Active Set.").

378. *Id.*, § 6.6.6.1.6, p. 6.71.

379. *See id.*, § 6.6.6.2.2, p. 6.78 (Listing the following data fields for the TrafficChannelAssignment message: MessageID, MessageSequence, ChannelIncluded, Channel, FrameOffset, DRCLength, DRCChannelGain, AckChannelGain, NumPilots, PilotPN, SofterHandoff, MACIndex, DRCCover, RABLength, RABOffset and a Reserved field.).

380. *Id.*, § 6.6.6.1.6.3.2, p. 6.72.

381. *Id.*, § 6.6.6.1.6.5, p. 6.73.

the access terminal."[382] "The access network should send a TrafficChannelAssignment message to the access terminal in response to changing radio link conditions, as reported in the access terminal's RouteUpdate messages."[383] "The access network should only specify a pilot in the TrafficChannelAssignment message if it has allocated the required resources in the associated sector. This means that the sector specified by the pilot is ready to receive data from the access terminal and is ready to transmit queued data to the access terminal should the access terminal point its DRC at that sector."[384] The process of an Access Terminal selecting a new Access Network is called a Connected State Route Update (*i.e.*, soft and hard handoffs)[385] and requires significant collaboration between the Access Terminal, the serving Access Network, the new Access Network, and the underlying packet data network.[386]

In order to not interrupt the Access Terminal user's Internet connection during a Connected State Route Update, the wireless carrier needs to use the A13 interface to transfer authentication and session configuration parameters from the current Access Network to the

382. *Id.*, § 6.6.6.1.6, p. 6.71.

383. *Id.*, § 6.6.6.1.6.3.1, p. 6.72.

384. *Id*.

385. *See* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 255 ("In 1X EV-DO the soft handoff is only supported in the reverse link and it follows a procedure very similar to cdma2000. In the forward link, however, there is no soft handoff and the network transmits the data only on the best sector selected by the AT on the DRC channel.").

386. *See id.*, p. 256 (explaining the Connected State Route Update process in the context of the air interface); ANSI/TIA-878-2, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network* (explaining the Connected State Route Update process in the context of the "underlying network," *i.e.*, the A13 interface).

new Access Network.[387] The A13 interface is a direct link between the current serving Access Network and the Access Network of which the Access Terminal is having its signal routed over the air interface.[388] The A13 interface is separate from the air interface used by the Access Network and Access Terminal to communicate via radio waves.[389] "The procedure for the A13 interface is a message flow to exchange AT and PDSN information between the ANs[]"[390] involved in a Connected State Route Update (*i.e.*, handoff). During a handoff, "[w]hen the target AN receives a packet from an AT that contains a UATI that is not in a subnet that is associated with the target AN, the target AN attempts to retrieve session related information from the source AN for the AT. The target AN sends an A13-Session Information Request message to the source AN to indicate the information requested. The target AN shall include the determined UATI, Security Layer Packet and Sector ID."[391] "When the source AN receives an A13-Session Information Request message it checks if the session information for

387. *See id.*, p. 265 ("In an enhanced 1X-EV DO system; different access networks can be connected to each other with an IOS-A13 interface defined within IOS [(*i.e.*, IS-878-2)]. This interface is required to support mobility procedures when the AT moves from one AN to another. The A13 interface allows the transfer of authentication and session configuration parameters from the old AN to the new AN. The interface is based on the UDP/IP and uses messages defined in the IOS.").

388. *See* ANSI/TIA-878-2, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 3.6.1, Figure 3.6.1-1, "Inter-PCF/Intra-PDSN Dormant AN-AN HO - Successful Operation," p. 3.15 (Connected State Route Update diagram showing the A13 interface directly linking two different Access Networks separate from the air interface).

389. *See id.*, § 2.4.1, p. 2.4 ("The IOS application is independent of the underlying physical transport medium, which is left to the discretion of operators and manufacturers.").

390. *Id.*, § 2.4.2, p. 2.4.

391. *Id.*, § 2.4.2.1.1, p. 2.5.

the requested AT exists and if it can authenticate the target AN request. After the source AN has successfully authenticated the message contained in the A13-Session Information Request message and has the requested session state information, it sends an A13-Session Information Response message to the target AN with the requested information."[392][393] Once the target AN receives the A13-Session Information Response message, the handoff is complete when "[t]he AT and the target AN complete the establishment of the HRPD session. Depending on the state of the AT and the target AN, either an existing HRPD session may be re-established, or a new HRPD session may be initiated if required."[394]

e. Open-loop and closed-loop power control of Access Terminal transmissions.

Regardless of implementation, all "CDMA base stations control the power of all mobiles for interference reduction purposes. All mobile signals must arrive at the base station at the same power level so that the signals can be properly coded. Power control is a required operational parameter of CDMA digital system operations."[395] In 1xEV-DO Rel. 0, "[t]he access terminal shall provide two independent means for output power adjustment: an open-loop estimation performed by the access terminal and a closed-loop correction involving both

392. *Id.*, § 2.4.2.2.1, p. 2.5.

393. In the alternative, if the source Access Network does not respond to the A13-Session Information Request message then "the target AN may begin a new session establishment with the AT." *Id.*, § 2.4.2.1.2, p. 2.5.

394. *Id.*, § 3.6.1(d), p. 3.16.

395. Bedell, *Cellular/PCS Management: A Real World Perspective*, p. 227.

the access terminal and the access network."[396] "In closed-loop power control, based on the measurement of the link quality, the base station sends a power control command instructing the mobile to increase or decrease its transmission power level. In open-loop power control, the mobile adjusts its transmission power based on the received signaling power from the base station."[397] The proceeding subsections explain the open-loop and closed-loop power control utilized by Access Terminals while sending reverse link transmissions to Access Networks.

i. Reverse Access Channel power control.

When establishing a session and opening a connection using the Access Probe process, open-loop power control is used to determine the power at which the Access Terminal transmits signals to the Access Network. As explained in Section III(B)(3)(c)(ii), *supra*, each Access Probe is an independent signal sent by the Access Terminal using both a pilot channel and data channel. In this context, the pilot channel and data channel make up the two part Reverse Access Channel with the pilot channel being sent first for a period of time (*i.e.*, the preamble) followed by the pilot channel and data channel being sent together for a period of time.[398] In order to calculate the mean transmit power used for the overall Reverse Access Channel, the Access Terminal measures the mean receive power of forward link signals broadcast by the Access Network and adds the negative of the resulting value to the values contained in the

396. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.2.4, p. 9.23.

397. Chuah *et al.*, *Design And Performance Of 3G Wireless Networks And Wireless LANs*, p. 7.

398. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.3.2, p. 9.34, Figure 9.2.1.3.2-1, "Example of an Access Probe."

OpenLoopAdjust and ProbeInitialAdjust data parameters broadcast by the Access Network via the AccessParameters message.[399][400][401] In order to determine the transmit power for each individual Access Probe sent as part of an Access sub-attempt, the Access Terminal multiplies the Access Probe number by the PowerStep value (provided to the Access Terminal via the AccessParameters message) and adds that value to the previously calculated mean transmit power used for the overall Reverse Access Channel.[402][403] During the preamble portion of any given Access Probe, the pilot channel is transmitted at the full calculated transmit power used for the Reverse Access Channel considering no data channel is transmitted.[404] During the data transmission portion of any given Access Probe, the Access Terminal uses the DataOffsetNom and DataOffset9k6 data parameter values (provided as public data of the Access Channel MAC Protocol) to determine the power at which to transmit the pilot channel and data channel.[405]

399. *See id.*, § 8.3.6.1.4.1.1, p. 8.25, No. 4 (providing mathematical equation).

400. The OpenLoopAdjust value sent to the Access Terminal by the Access Network contains "the nominal power to be used by access terminals in the open loop power estimate..." *Id.*, § 8.3.6.2.6, p. 8.32.

401. The ProbeInitialAdjust value sent to the Access Terminal by the Access Network contains "the correction factor to be used by access terminals in the open loop power estimate for the initial transmission on the Access Channel..." *Id*.

402. *See id.*, § 8.3.6.1.4.1.1, p. 8.25, No. 4 (providing mathematical equation).

403. The PowerStep designates "the increase in power between probes, in resolution of 0.5 dB." *Id.*, § 8.3.6.2.6, p. 8.32.

404. *See id.*, § 9.2.1.3.2, p. 9.34 ("The output power of the Pilot Channel during the preamble portion of an access probe is higher than it is during the data portion of the probe by an amount such that the total output power of the preamble and data portions of the access probe are the same as shown in Figure 9.2.1.3.2-1.").

405. *See id.*, § 9.2.1.2.4.1, p. 9.23-9.24.

When data is being transmitted, the combined transmit power of the pilot channel and data channel total the full calculated transmit power used for the Reverse Access Channel.[406] While engaging in Access Attempts as explained in Section III(B)(3)(c)(ii), *supra*, the Access Terminal uses the open-loop power control process explained above.

ii. Reverse Traffic Channel power control.

After a connection is open and a Reverse Traffic Channel assigned to the Access Terminal by the Access Network,[407] a combination of open-loop and closed-loop power control is used to determine the power at which the Access Terminal transmits signals to the Access Network.[408] "When the access terminal is transmitting the Reverse Traffic Channel, the access terminal transmits the Pilot Channel, the DRC Channel, the ACK Channel when acknowledging received physical layer packets, and the Data Channel when transmitting physical layer packets. These channels shall be transmitted at power levels according to open-loop and closed-loop power control."[409] For the initial open-loop power estimate, "[t]he initial mean output power of the Pilot Channel of the Reverse Traffic Channel shall be equal to the

406. *See id*.

407. While communicating with the Access Network after a Reverse Traffic Channel is assigned, the Access Terminal configures its transmissions using various well known fall-back data values or data values as designated by the Access Network via ConfigurationRequest messages (sent according to the the Generic Configuration Protocol) containing attributes including the PowerParameters Attribute and the RateParameters Attribute (both of which contain numerous data fields and records sent to and stored by the Access Terminal). *See id.*, § 8.5.7, p. 8.79-8.84.

408. *See id.*, § 9.2.1.2.1.2, p. 9.22 ("When the access terminal is transmitting the Reverse Traffic Channel, the access terminal shall control the mean output power using a combination of closed-loop and open-loop power control...").

409. *Id.*, § 9.2.1.2.1.2, p. 9.22-9.23.

mean output power of the Pilot Channel at the end of the last Access Channel probe minus the difference in the forward link mean received signal power from the end of the last Access Channel probe to the start of the Reverse Traffic Channel transmission."[410] "During the transmission of the Reverse Traffic Channel, the determination of the output power needed to support the Data Channel, the DRC Channel, and the ACK Channel is an additional open-loop process performed by the access terminal."[411][412] This process utilizes the DataOffsetNom, DataOffset9k6, DataOffset19k2, DataOffset38k4, DataOffset76k8, DataOffset153k6, DRCChannelGain, and ACKChannelGain data parameter values (provided as public data of the Reverse Traffic Channel MAC Protocol) to determine the power at which to transmit the various noted channels relative to the mean output power of the pilot channel.[413] The subsequent mean output power of the reverse link pilot channel is dictated by the Access Network through closed-loop power control. "For closed-loop correction (with respect to the open-loop estimate), the access terminal shall adjust the mean output power level of the Pilot Channel in response to each power-control bit received on the Reverse Power Control (RPC)

410. *Id.*, § 9.2.1.2.4.1, p. 9.24.

411. *Id.*

412. *See also* Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 255 ("The reverse power control is directly applied to the pilot/RRI channel only, and the power levels allocated to the DRC, ACK, and data channels are adjusted by a fixed gain relative to the pilot/RRI channel. The channel gains are defined based on the coding gain, the target reliability, and the data rate for each channel to achieve the desired performance.").

413. *See* TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.2.4.1, p. 9.24-9.25.

Channel."[414] Whenever a connection is open, "the access network continuously transmits '0' (up) or '1' (down) RPC bits to the access terminal, based on measurements of the reverse link signal quality. If the received quality is above the target threshold, a '1' bit is transmitted. If the received quality is below the target threshold, a '0' bit is transmitted."[415] Through commands sent to the Access Terminal over the air interface, the Access Network is able to increase or decrease the Access Terminal transmit power at least ±24 dB around the Access Terminal's open-loop transmit power estimate.[416]

f. Synchronization and timing of transmitted signals.

"All sector air interface transmissions are referenced to a common system-wide timing reference that uses the Global Positioning System (GPS) time, which is traceable to and synchronous with Universal Coordinated Time (UTC)."[417][418] Based on the GPS time maintained by the Access Network, the Access Terminal establishes "a time reference that is

414. *Id.*, § 9.2.1.2.4.2, p. 9.25.

415. *Id.*, § 9.2.1.4, p. 9.53.

416. *See id.*, § 9.2.1.2.4.2, p. 9.26.

417. *Id.*, § 1.14, p. 1.17.

418. *See also* USDOD, *Global Positioning System Standard Positioning Service Performance Standard* (4th ed. 2008), Appendix C, p. C-2 ("GPS Time. A continuous time scale maintained by the GPS Control Segment which began at midnight on the night of 5/6 January 1980 on the Coordinated Universal Time (UTC) scale as established by the U.S. Naval Observatory (USNO)"); Smithsonian: National Air and Space Museum [website], *How Does GPS Work?*, http://www.nasm.si.edu/exhibitions/gps/work.html (last accessed: Dec. 1, 2011) ("GPS operations depend on a very accurate time reference, which is provided by atomic clocks at the U.S. Naval Observatory. Each GPS satellite has atomic clocks on board.").

used to derive timing for the transmitted chips, symbols, slots, frames, and system timing."[419] "The access terminal initial time reference shall be established from the acquired Pilot Channel and from the Sync message transmitted on the Control Channel."[420] In other words, through the Pilot Channel and Sync message, the Access Network instructs the Access Terminal to transmit signals only at specific time intervals. Because the Access Terminal time reference is "used as the transmit time reference of the Reverse Traffic Channel and the Access Channel[,]"[421] the Access Network always knows the time at which the Access Terminal transmits a signal. For example, "The Access Channel Cycle specifies the time instants at which the access terminal may start an access probe."[422] Similarly, the Access Network transmits to the Access Terminal at specified times.[423] For example, "[t]he AN sends the broadcast and common channel messages on the control channel slots in every 256 slots = 426.67 ms."[424]

419. TIA/EIA/IS-856-1, *cdma2000 High Rate Packet Data Air Interface Specification*, § 9.2.1.6, p. 9.54.

420. *Id*.

421. *Id*.

422. *Id.*, § 8.3.6.1.2, p. 8.22.

423. *See* Korowajczuk, *Designing cdma2000 Systems*, p. 396 ("The AN (sector) also uses the system time as a reference for all its time-critical transmission components, including pilot PN sequences, slots and Walsh functions.").

424. Etemad, *cdma2000 Evolution: System Concepts and Design Principles*, p. 238.

g. Relevant miscellaneous 1xEV-DO Rel. 0 cellular data network operations.

i. Signal interference.

All cellular systems, including those supporting 1xEV-DO Rel. 0, are susceptible to signal interference on the air interface. The FCC defines signal interference as "[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."[425] "Interference usually occurs between two radio signals whose frequencies are too close together, or even identical."[426] Two common types of interference in a cellular network are cochannel interference and adjacent channel interference. "Cochannel interference occurs when there are two or more transmitters within a cellular system, or even a neighboring cellular system, that are transmitting on the *same* frequency (channel). This type of interference is usually generated because channel sets have been assigned to two cells that are *not far enough apart*; their signals are strong enough to cause interference to each other."[427] "Adjacent channel interference is caused by the *inability* of a mobile phone to filter out the signals (frequencies) of adjacent channels assigned to side-by-side cell sites []."[428] "There are other types of interference that occasionally plague cellular systems. The most common form of interference, other than cochannel and adjacent channel interference, is

425. 47 C.F.R. § 2.1(c).

426. Bedell, *Cellular/PCS Management: A Real World Perspective*, p. 43.

427. *Id*.

428. *Id.*, p. 45.

intermodulation interference (IM)."[429] "Intermodulation interference describes the effect of several signals mixing together to produce an unwanted signal, or even no signal at all."[430]

In order to avoid signal interference on the air interface, wireless carriers implement frequency coordination defined as "the effort to assign frequencies to cellular channels in such a way as to minimize interference within your *own* cellular system and *neighboring* systems of different wireless carriers."[431] Wireless carriers use both intramarket and intermarket frequency coordination. Intramarket frequency coordination is done internally by each wireless carrier and "is based on a frequency-reuse growth plan using the hex grid."[432] "The configuration and planning of [][each cell within the hex grid] is chosen to minimize the interference from another cell and thus maximum capacity can be achieved."[433] Intermarket frequency coordination "is external to a wireless carrier's cellular system, and involves coordinating frequency assignments with neighboring cellular systems[]."[434] "The FCC dictates that all reasonable actions must be taken to limit and/or reduce interference between two cellular systems."[435] For example, the FCC requires that "[l]icensees in the Cellular Radiotelephone Service must coordinate, with the appropriate parties, channel usage at each

429. *Id*.

430. *Id*.

431. *Id*.

432. *Id.*, p. 42.

433. Chuah *et al.*, *Design And Performance Of 3G Wireless Networks And Wireless LANs*, p. 2.

434. Bedell, *Cellular/PCS Management: A Real World Perspective*, p. 42.

435. *Id*.

transmitter location within 121 kilometers (75 miles) of any transmitter locations authorized to other licensees or proposed by tentative selectees or other applicants, except those with mutually exclusive applications."[436] Additionally, the FCC has strict guidelines that must be followed by wireless carriers to prevent and correct network issues that cause interference with 800mhz Public Safety Radio Service,[437] *i.e.*, radios used by ambulances, firefighters, police officers, *etc*.

ii. Hybrid Access Terminal operations for non-telephones, *e.g.*, aircards.

As explained in Section III(B)(2)(a), *supra*, most Access Terminals are hybrid Access Terminals (HATs) meaning they are capable of communicating with both 1xEV-DO cellular data networks and 1xRTT cellular data/voice networks. An example of a HAT that supports all connection types across both networks (*i.e.*, 1xEV-DO high speed Internet, 1xRTT low speed Internet, 1xRTT telephone calls, and 1xRTT SMS text messages) is a "smart phone."[438] An example of a HAT that supports 1xEV-DO data connections and 1xRTT data connections (but

436. 47 C.F.R. § 22.907; *see also* 47 C.F.R. § 22.351 ("All applicants for, and licensees of, stations in the Public Mobile Services shall cooperate in the selection and use of channels in order to minimize interference and obtain the most efficient use of the allocated spectrum.").

437. *See* 47 C.F.R. § 22.970 *et seq.*; 47 C.F.R. § 22.971(a) ("Any licensee who, knowingly or unknowingly, directly or indirectly, causes or contributes to causing unacceptable interference to a non-cellular part 90 [(*i.e.*, Public Safety Radio Service)] of this chapter licensee in the 800 MHz band, as defined in § 22.970, shall be strictly accountable to abate the interference, with full cooperation and utmost diligence, in the shortest time practicable.").

438. "Smart Phone: Wireless phones with advanced data features and often keyboards. What makes the phone 'smart' is its ability to better manage data and Internet access." CTIA [website], *Wireless Glossary of Terms Q-S*, http://www.ctia.org/media/industry_info/index.cfm/AID/10406 (last accessed: Aug., 30, 2011).

not voice connections) is an aircard that plugs into a host laptop computer.[439] In the context of an aircard, support for 1xRTT provides an SMS text message service and low speed Internet access in places where 1xEV-DO High Rate Packet Data (HRPD) service is unavailable. Hybrid Access Terminals should not be confused with SVDO Access Terminals.[440] Hybrid Access Terminals allow for data connections via 1xEV-DO air links or a data and/or voice connection via 1xRTT air links, but not at the same time.[441] In contrast, SVDO Access Terminals allow for *simultaneous* 1xEV-DO and 1xRTT air links with traffic channels assigned for each link.[442][443] In the context of an SVDO Access Terminal consisting of hardware capable of supporting voice calls, if a 1xEV-DO data connection is open during the time of an incoming voice page, the Access Terminal stays in the connected state (*i.e.*, no impact on 1xEV-DO data session) while it utilizes separate radio channels to connect the incoming voice call.[444] In contrast, a voice capable Hybrid Access Terminal under the same scenario will drop

439. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (government web research on aircard).

440. SVDO Access Terminals were not being marketed in the year 2008.

441. *See* TIA-1157-A, *Signaling Conformance Test Specification for Interworking of CDMA2000 1X and High Rate Packet Data Systems, Revision A*, § 1.2, p. 1.1 (A Hybrid Access Terminal is a "[h]ybrid mode device that can support cdma20001x [(*e.g.*, 1xRTT)] and HRPD [(*e.g.*, 1xEV-DO)] by periodic monitoring [of] the paging channel of cdma20001x.").

442. *See id*.

443 The simultaneous voice and data operation of an SVDO Access Terminal should not be confused with the "concurrent services" operation of a Hybrid Access Terminal using solely 1xRTT to concurrently access low speed Internet and a voice call.

444. *See id.*, § 3.6, p. 3.4-3.5 (Outlining test guidelines to "verif[y] a voice call termination in active HRPD mode for SVDO capable AT.").

the 1xEV-DO air link (if the user chooses to answer the call) so that resources are freed to connect the incoming voice call on the 1xRTT system.[445]

The technical standard labeled IS-878-2 provides instructions on how a Hybrid Access Terminal handles incoming 1xRTT voice calls (via pages) under various scenarios while in "Active Mode," *i.e.*, having an open 1xEV-DO data connection.[446][447] Under a scenario applicable to "concurrent services," if a voice capable Hybrid Access Terminal receives a 1xRTT page from a Base Station (indicating an incoming voice call) while engaged in an open 1xEV-DO data connection with an Access Network, the Access Terminal will (1) stop transmitting to the Access Network, (2) respond to the page by communicating with the Base Station over the air interface, (3) receive an "Alert with Info" message from the Base Station instructing the telephone hardware to ring, and (4) have its 1xEV-DO packet data session handed off to the 1xRTT system for concurrent call/data services (*i.e.*, low speed Internet and voice simultaneously).[448] During the above explained process, the Base Station will establish a 1xRTT packet data session to take the place of the previous 1xEV-DO packet data session so

445. *See id.*, § 3.2, p. 3.1-3.2 (Outlining test guidelines to "verif[y] a voice call termination when in HRPD Active Mode.").

446. *See* ANSI/TIA-878-2, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 4.2 *et seq.*, p. 4.7.

447. An Access Terminal "is in Active Mode when it has a session established with an HRPD system, a PPP session established and an air-interface connection open with the HRPD system." TIA-1157-A, *Signaling Conformance Test Specification for Interworking of CDMA2000 1X and High Rate Packet Data Systems, Revision A*, § 1.6, p. 1.2.

448. *See* ANSI/TIA-878-2, *Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network*, § 4.2.1, p. 4.7-4.9 & Fig. 4.2.1-1.

that Internet access will be maintained while the voice call is in progress.[449] Under a similar scenario but applicable to Access Terminals with **no** support for "concurrent services," the same first three steps are completed but no request will be made to handoff the 1xEV-DO packet data session to the 1xRTT network.[450] Under this variant, the Access Network starts a "$T_{airdrop}$" timer and releases the entire 1xEV-DO session if it does not receive a 1xEV-DO transmission from the Access Terminal within a period of time ranging from 0.1 to 60.0 seconds as set by the wireless carrier.[451] If the user of the Hybrid Access Terminal answers the ringing phone, the Access Network's timer eventually runs out and it closes the Access Terminal's PPP session established with the PDSN and its HRPD session established with the Access Network.[452] If the call is not answered by the Access Terminal user, the Access Terminal resumes transmissions over the 1xEV-DO air link and the 1xEV-DO connection resumes.

Regardless of whether concurrent services are supported, none of the above applies to Hybrid Access Terminals that do not support voice calls (*e.g.*, aircards). A factory set Hybrid Access Terminal lacking telephone hardware will ignore 1xRTT pages resulting from typical incoming voice calls and the 1xEV-DO data connection will not be disrupted. Under both

449. *See id*.

450. *See id.*, § 4.2.2, p. 4.10-4.11 & Fig. 4.2.2-1.

451. *See id.*, § 5.3, p. 5.10 (Showing $T_{airdrop}$ timer with s default value of 5 seconds and a possible range of 0.1-60.0 seconds); § 5.3.1.1 ($T_{airdrop}$ is an Access Network timer indicating "when an HRPD connection has been lost. The timer is started by the AN when it determines that it is not receiving any transmissions from the MS/AT and stopped when the AN resumes receiving transmissions from the MS/AT or upon receipt of the A9-Disconnect-A8 message.").

452. *See id.*, § 4.2.2, p. 4.10-4.11 & Fig. 4.2.2-1.

scenarios explained above, the IS-878-2 technical standard states that "[t]he MS/AT may ignore this Page Message to continue the HRPD session. If the MS/AT ignores the message, the following steps are not performed."[453] Because non-telephone Hybrid Access Terminals have no reason to respond to 1xRTT pages for voice calls, let alone issue connect orders for the calls, they ignore all incoming telephone calls and never even reach the first step of ceasing transmissions to the Access Network.

C. Explanation of the term "triangulation" applicable to geolocation of radio frequency (RF) signals.

"In navigation, surveying, and civil engineering, triangulation is a technique for precise determination of a ship's or aircraft's position, and the direction of roads, tunnels, or other structures under construction. It is based on the laws of plane trigonometry, which state that, if one side and two angles of a triangle are known, the other two sides and angle can be readily calculated."[454] However, in the context of geolocating wireless devices via radio signals,[455] the meaning of triangulation has evolved into a generically used term encompassing any

453. *See id.*, § 4.2.1, p. 4.8 (a); *id.* § 4.2.2, p. 4.10 (a);

454. Hosch, William L., ed., *The Britannica Guide to Algebra and Trigonometry*, (New York, NY: Britannica Educational Publishing, 2011), p. 266-67.

455. "*Geolocation* of RF signals is defined as the problem of precise localization (or geolocation) of spatially separated sources emitting electromagnetic energy in the form of *radio signals* within a certain frequency bandwidth by observing their received signals at spatially separated sensors (or array elements) of the geolocation of RF signals system... *Geolocation of RF signals* is of considerable importance occurring in many fields, including radar, sonar, mobile communications, radio astronomy, seismology, unmanned air vehicle (UAV) for intelligence gathering information, emergency and rescue personnel, mining and agriculture, drilling, aviation, ground transportation, naval, *etc.*" Progri, Ilir, *Geolocation of RF Signals: Principles and Simulations* (New York, NY: Springer, 2011), p. 5.

number of radio signal measurements taken at two or more collection points (simultaneity is **not** required) where radio signals are received from a wireless device.[456] Triangles, angles, and stationary measurement points (as are needed in traditional triangulation) are not necessary elements of radio signal triangulation. Inventors of wireless device locating technology use the term "triangulation" to generically refer to any number of geolocation measurement techniques used to locate wireless devices.[457] For example, Bromhead *et al.*, inventors of wireless device geolocation technology, applied the term "triangulate" in reference to using signal power levels and signal timing measurements as a way to locate a wireless device.[458] Hildebrand *et al.* (Harris), inventors of wireless device geolocation technology, explained "triangulation" as using two receivers to determine radio signal angle of arrival and time difference of arrival to locate a cellular device.[459] Dupray *et al.*, inventors of *Geographic Location Using Multiple*

456. *See*, *e.g.*, *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 2nd sess. (Jun. 24, 2010), APPENDIX, "Materials Submitted for the Hearing Record" (Written Responses of Matt Blaze), p. 138 (PDF, p. 142) ("'Triangulation' in this context refers to a range of techniques for more precisely locating a cellular subscriber handset by comparing the radio signal received from the handset at multiple vantage points.").

457. Even traditional "triangulation" sometimes adopts a broader generic meaning that encompasses "trilateration." *See* Morris, Christopher G., ed., *Academic Press Dictionary of Science and Technology*, (San Diego, CA: Gulf Publishing Group, 1992), p. 2265 (Defining "**trilateration**" as "a method of land surveying that uses triangulation to measure the distance between a series of points on the earth's surface.").

458. *See* Bromhead, Nicholas and McCarthy, Mathtew N., *Sub-Sector Timing Advance Positions Determinations*, U.S. Patent App. No. 2004/0203921 (Thornbury, AU: Oct. 14, 2004), *available at* http://www.freepatentsonline.com/y2004/0203921.html (last accessed: Sept. 29, 2010), p. 2, ¶ 12 ("**Signal power** level or **signal timing** measurements between the mobile terminal and three or more base stations are used to **triangulate**." (emphasis added)).

459. *See* Hildebrand, Robert C., *et al.*, Harris Corp., *Geolocation Of Cellular Phone Using Supervisory Audio Tone Transmitted From Single Base Station*, U.S. Patent No. 6,292,665 (Indialantic: Sept. 18, 2001), *available at* http://www.freepatentsonline.com/6292665.html (last

Location Estimators, used the term "triangulation" while explaining GPS.[460][461] Recent technical texts and papers also use "triangulation" to refer to measurements of distance, time, signal power, and signal direction.[462][463] In sum, triangulation refers to use of one or more of the following geolocation techniques: (1) time-of-flight (TOF) (a.k.a time-of-arrival), (2) time-

accessed: Feb. 16, 2011), p. 1, ln. 46-49 ("Other proposals include the use of a phased array antenna and a pair of receiver stations to determine **angle of arrival** and difference in **time of arrival** for **triangulation** purposes." (emphasis added)).

460. *See* Dupray, Dennis J., *et al.*, TracBeam, LLC, *Geographic Location Using Multiple Location Estimators*, U.S. Patent No. 7,298,327 (Golden, CO (US): Nov. 20, 2007), *available at* http://www.freepatentsonline.com/7298327.html (last accessed: Feb. 22, 2011), p. 1, ln. 60-63 ("Another example of a location system using time of arrival and **triangulation** for location are satellite-based systems, such as the military and commercial versions of the Global Positioning Satellite system ('GPS')." (emphasis added)).

461. Pop-culture fiction novelist, Tom Clancy, also entertains his readers with a generic triangulation concept that encompasses GPS. *See* Preisler, Jerome, *Tom Clancy's Power Play: Zero Hour*, (New York, NY: Berkley Publishing Group, 2003) p. 239 ("Bottom-of-the-line [GPS] units lock on to three sats and provide a two-dimensional fix on position—latitude and longitude. The coordinates are arrived at by simple **triangulation**...the travel time of the satellite signals beamed to the receiver times the speed of light [(*i.e.*, **time-of-flight**)]." (emphasis added)).

462. *See*, *e.g.*, Dwivedi, Himanshu *et al.*, *Mobile Application Security*, (McGraw-Hill (USA 2010), p. 332 (Explaining "Tower **Triangulation**" as using the "relative **power levels** of radio signals between a cell phone and a cell tower of a known location..." (emphasis added)).

463. *See*, *e.g.*, The House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection and Subcommittee on Communications, Technology, and the Internet, *The Privacy Implications of Commercial Location-Based Services*, 111th Cong. (Feb. 24, 2010) (Statement by John B. Morris, Jr., General Counsel, and Director of CDT's Internet Standards, Center for Democracy & Technology), *available at* hhttp://democrats.energycommerce.house.gov/Press_111/20100224/Morris.Testimony.2010.02.24.pdf (last accessed: Apr. 9, 2012), p. 4. ("[I]f two or three cell towers can detect a mobile device at the same time, the carrier can triangulate from the towers to determine the approximate location of the phone... [and] if needed, make calculations based on the **strength**

difference-of-arrival (TDOA), (3) angle-of-arrival (AOA), and (4) power-distance.[464] Various geolocation techniques are further discussed *infra*.

For radio wave collection purposes, the traditional triangulation requirement of needing two stationary points taking measurements simultaneously can also be written out of the triangulation equation through use of the "approach" method.[465] Instead of using multiple stationary wireless device locators, such as wireless carrier cell sites, a portable/transportable wireless device locator can use the approach method to take numerous triangulation calculations from multiple vantage points. In referencing this method, the USDOJ Electronic Surveillance Manual states that "[l]aw enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones[, and b]y **shifting the location of the device**, the operator can determine the phone's location more precisely using **triangulation**."[466] Through a different method using multipath signals, a stationary wireless device locator, such as a wireless carrier cell site, can autonomously triangulate the location of a wireless device.[467] A single stationary wireless device locator can triangulate by collecting

---

and **direction** of a phone's signal..." (emphasis added)).

464. Other elements of geolocation involve applying received signal measurements, statistical functions, and data fusion to multiple triangulation calculations for increased accuracy; and Doppler measurements for ascertaining velocity of a wireless device. Each of these geolocation elements is further discussed *infra*.

465. The approach method is further explain in the *Technical Explanations*, Section III(G)(1)(b)(v), *infra*.

466. U.S. Dep't of Justice, *Electronic Surveillance Manual*, p. 45 (emphasis added). *See also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 052 of *2nd Consolidated Exhibits* (Dkt. #821-3) (section on cell site emulators, *etc.*, p. 40-41 and 44-45).

467. *See* Holt, Brian, Harris Corp., *Method And System For Calibrating Wireless Location*

and measuring multipath signals reflected from proxy receivers such as water towers, hillsides, or other natural or man-made objects.[468] The proxy receiver method is unique in that it allows for a single wireless device locator in a stationary position to conduct triangulation measurements on radio signals as if being done by multiple wireless device locators in stationary positions or by a single portable/transportable wireless device locator engaged in the approach method.

D. Cell site information and its use in geolocating wireless devices.

1. Explanation of the term "cell site information."

Cell site information may be generated by a wireless carrier when a wireless device accesses a cell site over the air interface. The term "cell site information" is an ambiguous catch-all phrase referring to many different subsets of data generated in response to a wireless device accessing a cell site such as a 1xEV-DO Rel. 0 Access Network.[469] The different subsets of data making up cell site information are dictated by various elements such as cellular

Systems, U.S. Patent No. 6,795,019 (Melbourne, FL: Sept. 21, 2004), *available at* http://www.freepatentsonline.com/6795019.html (last accessed: Feb. 16, 2011), p. 4, ln. 52-54 ("The present invention is advantageous and allows the use of **one** receiver at a receive site to determine the location of a mobile transmitting unit..." (emphasis added)).

468. *See id.*, p. 4 ln. 56-66 ("The system uses a proxy receiver (or passive reflector) for Time of Arrival and/or Time of Difference of Arrival calculations. Throughout the description, the term proxy receiver is used for a reflector/refractor located at a location called a proxy receive site (PRS) and also used to describe any type of passive reflector, such as a building, mountain, or hill, water tower, or any other natural or man-made object that would reflect and/or refract (or diffract) the signal from a transmitting mobile unit or other radio transmitter to a receiver that could be fixed or mobile.").

469. A wireless carrier may generate and store cell site information for later law enforcement use (*i.e.*, historical cell site information) or forwarded it to law enforcement in real-time (*i.e.*, real-time cell site information).

network infrastructure, service features, wireless device type, and cell site design. In the context of historical cell site information, the subset of cell site information making up *location* information is not standardized across wireless carriers. "Some providers may collect only information about the nearest tower [(either with or without sector information)]... [and] how revealing th[at] is depends on the density of the area in which the subscriber is located. Other providers, however, may collect more precise information and may collect location records at more frequent intervals, which might reveal, for example, not only a subscriber's individual locations but also his or her direction and rate of travel, travel habits, and other patterns of behavior."[470]

An analysis of historical cell site information provided by wireless carriers in three separate cases demonstrates the ambiguous, catch-all nature of the term. In United States v. Luis Soto, Sprint Nextel Corporation provided historical cell site information consisting of the following data fields: (1) Date; (2) Time; (3) Duration (sec); (4) FromUrbanArea NetworkCode; (5) FromACGId; (6) Destination UFMI; and (7) Direct Connect Number. *See id.*, Case No. 3:09-cr-00200-AWT, Doc. #112-1 (D. Conn., Jun. 28, 2010); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 110 of *2nd Consolidated Exhibits* (Dkt. #821-6) (cell site information record attached). In The Matter Of An Application Of The United States Of America For An Order Authorizing The Release Of Historical Cell-

470. *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 2nd sess. (Jun. 24, 2010), APPENDIX, "Materials Submitted for the Hearing Record" (Written Responses of Matt Blaze, Associate Professor, University of Pennsylvania, on ECPA Reform, August 20, 2010), p. 135 (PDF, p. 139).

Site Information, an unknown wireless carrier provided historical cell site information consisting of the following data fields: (1) Customer PTN; (2) Date; (3) Call Initiation Time; (4) Duration (sec); (5) Type; (6) Forwarded; (7) 911; (8) International; (9) Caller / Called PTN; (10) Originating Cell Site; and (11) Terminating Cell Site. *See id.*, Case No. 1:10-mc-00550-RRM-JO, Doc. #004-2 (E.D.N.Y., Aug. 24, 2010); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 111 of *2nd Consolidated Exhibits* (Dkt. #821-6) (cell site information record attached). Finally, in the present case, Verizon Wireless provided historical cell site information consisting of the following data fields: (1) Details; (2) MDN; (3) MSID; (4) Cell Start Date/Time; (5) Event Stop Date/Time; (6) Duration (seconds); (7) MOU; (8) KBU; (9) SID; (10) Mscid; (11) Cell; (12) Switch; (13) Cell #; (14) LAT; (15) LONG; (16) ADDRESS; (17) CITY; (18) STATE; and (19) ZIP. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 03 of *1st Consolidated Exhibits* (Dkt. #587-1).[471]

2. Use of statistical databases containing historical cell site location information to determine a wireless device location signature.

There are various ways to use statistical databases containing historical cell site location information to determine the past, present, and future location of a wireless device. By using information about the terrain and received signals collected over time (*i.e.*, historical cell site

471. *See also* In Re Application For Pen Register And Trap/trace Device With Cell Site Location Authority, 396 F.Supp.2d 747, 749 (S.D.Tex. 2005) ("Smith (mj) 2005 Opinion") (Defining *real-time* (*i.e.*, prospective) cell site information as "the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls)..." and "information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture.").

location information), a wireless carrier or law enforcement can use heuristics to ascertain the location signature of a wireless device. "In one embodiment, the PDE [(*i.e.*, Position Determination Entity)] may collect statistical data about the reported PN phases from any [] [wireless device], organized within small geographic regions surrounding a [][cell site].... With a sufficient number of phase measurement samples, the PDE can make general assumptions about the multipath environment within a given region, measured by a plurality of [][wireless devices]..."[472] The phase measurement samples (*i.e.*, historical cell site location information) are entered into a statistical database[473] used to divide each cell site coverage area into regions that correspond to the available location signatures.[474] In U.S. Patent No. 6,999,778, DiBuduo provides a diagram showing five regions surrounding a cell site with each region corresponding to a different location signature.[475] If a wireless carrier needs to determine the region where a wireless device is located, it compares cell site location information corresponding to the target

472. DiBuduo, Marcus, Denso Corp., *Multipath Assistance For Pilot Phase Measurement Processes*, U.S. Patent No. 6,999,778 (Oceanside, CA: Feb. 14, 2006), *available at* http://www.freepatentsonline.com/6999778.html (last accessed: Sept. 29, 2010), p. 7, ln. 44-46 and 49-52 (for clarity and consistency purposes, the terms "BS" (Base Station) are changed to "cell site" and "MS" (Mobile Station) to "wireless device").

473. *See id.*, p. 12, ln. 61-65 ("[T]his statistical database can be generated by considering any information provided to the PDE in the PPM. Over time, the PDE will compile previously reported pilot phase measurements from multiple MSs in a particular region and create the statistical distribution...").

474. *See id.*, p. 11, ln. 33-38 ("The statistical database compiled by the PDE can be divided into multiple regions for each BS. FIG. 10 is a diagram showing five regions surrounding BS A for which a database consisting of received PPMs from MSs located within those regions is maintained according to the present invention.").

475. *See id.*, Sheet 9 of 11, Fig. 10; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 057 of *2nd Consolidated Exhibits* (Dkt. #821-3) (Fig. 10 attached).

wireless device to entries in the statistical database in order to obtain a location signature match.[476]

In another embodiment, Dupray *et al.* explains a system that collects historical location data to establish location signatures "based on: (a) the terrain area classifications; *e.g.*, the terrain of an area surrounding a target MS, (b) the configuration of base stations in the radio coverage area, and (c) characterizations of the wireless signal transmission paths between a target MS location and the base stations."[477] Dupray *et al.* employs a real number confidence value system to weight specific geographic areas according to the probability of containing the target wireless device (*i.e.*, the MS). "That is, confidence values that are larger indicate a higher likelihood that the target MS is in the corresponding MS estimated area, wherein -1 indicates that the target MS is absolutely NOT in the estimated area, 0 indicates a substantially neutral or unknown likelihood of the target MS being in the corresponding estimated area, and 1 indicates that the target MS is absolutely within the corresponding estimated area."[478] In summary, the invention by Dupray *et al.*, "provide[s] location hypothesis enhancing and evaluation techniques that can adjust target MS location estimates according to historical MS

476. *See id.*, p. 17, ln. 30-31 (claiming that the invention allows for locating a wireless by "estimating a location of the MS using PN phase offsets previously reported by the MS;").

477. Dupray, *et al.*, TracBeam, LLC, *Geographic Location Using Multiple Location* Estimators, U.S. Patent No. 7,298,327, p. 43, ln. 41-46 (claim notes omitted); *see also id.*, p. 15 ln. 62-67, p. 16 ln. 1 ("A novel aspect of the present invention relies on the discovery that in many areas where MS location services are desired, the wireless signal measurements obtained from communications between the target MS and the base station infrastructure are extensive enough to provide sufficiently unique or peculiar values so that the pattern of values alone may identify the location of the target MS.").

478. *Id.*, p. 14, ln. 60-67.

location data and/or adjust the confidence values of location hypotheses according to how consistent the corresponding target MS location estimate is..."[479]

3. Cell site triangulation of a wireless device using cell site location information.

There are various geolocation techniques that can be used to triangulate a wireless device using cell site location information. The most basic form of cell site triangulation uses low resolution angle-of-arrival (AOA) measurements taken from two overlapping cell site sectors belonging to adjacent cell sites:

> Triangulation is the process of determining the coordinates of a point based on the known location of two other points. If the direction (but not distance) from each known point to the unknown point can be determined, then a triangle can be drawn connecting all three points. While only the length of one side of the triangle is known at first (the side connecting the two known points), simple trigonometry reveals the lengths of the other sides and so the position of the third point. **In the context of cell site information**, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is discerned from the information about which face of each tower is facing the phone.
>
> In Re: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp.2d 448, 451 (S.D.N.Y. 2006) (district Judge Kaplan) (emphasis added).

For the type of cell site triangulation explained above, the 120° cell site sectors[480] make up the angles used in the angle-of-arrival (AOA) measurements. Therefore, the minimum amount of

479. *Id.*, p. 15, ln. 2-7.

480. Typical cell sites, including the cell sites accessed by the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.), had three 120° sectors providing cellular service. *See Technical Explanations*, Section III(B)(2)(c), *supra* (explaining cell sites in the geolocation context); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map showing three tri-sectored cell sites that were accessed by the aircard).

cell site location information needed for triangulation is information identifying each sector accessed by the wireless device. Angle-of-arrival (AOA) measurements in this context are considered low resolution because a sector having a radiation pattern oriented at 120° with center azimuth bearing at 60° is only capable of locating a wireless device at a vector angle centered at 60° with a line bearing uncertainty of 120°. Therefore, the line bearing pointing to the location of the wireless device is somewhere along a set 120° arc as part of a 360° circle with the cell site hardware at the center of the circle. However, because line bearings are measured from two separate cell site sectors, the level of location uncertainty is reduced to an area where the two cell site sectors overlap.[481]

More precise forms of cell site triangulation are also employed—mainly in real-time by wireless carriers seeking to "compl[y] with the FCC's 'E911' mandate for more precisely locating cellular callers to emergency services. When a subscriber places a call to 911, many cellular networks automatically employ some form of triangulation and automatically transmit the calculated location of the caller to the 911 call center."[482] However, high resolution geolocation information may also be continuously compiled by wireless carriers for law

481. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map showing how triangulation via cell site sector angle-of-arrival (AOA) measurements in combination with location signature techniques eliminated **93.9%** of the location uncertainty); *see also How The Aircard Was Intruded Upon*, Section IV(B)(2), *infra* (explaining the precise techniques used to created the cell tower range chart/map).

482. *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 2nd sess. (Jun. 24, 2010), APPENDIX, "Materials Submitted for the Hearing Record" (Written Responses of Matt Blaze), p. 138 (PDF, p. 142).

enforcement use—even while 911 calls are not involved.[483] In order to conduct high resolution geolocation of a wireless device, wireless carriers use various network-based triangulation techniques including time-of-flight (TOF), time-difference-of-arrival (TDOA), angle-of-arrival (AOA), and power-distance. For network based geolocation, triangulation calculations are conducted by cell sites in combination with other network hardware and may also involve handset based measurements of cell site pilot signals as recorded by the wireless device.[484][485][486] According to E911 requirements, network-based geolocation techniques will have a sufficient resolution if they are accurate to "100 meters for 67 percent of calls, [and] 300

483. For example, TruePosition's network-based geolocation product not only serves E911 purposes, it also serves a law enforcement need for "safe shared and secure access to definitive information relating to the size, detail, location and activity of illegal conduct." *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of Michael Amarosa, Senior Vice President, TruePosition, Inc.), p. 44 (PDF, p. 48).

484. *See* Caffery, James J., Jr. and Stüber, Gordon L., Georgia Institute of Technology, *Overview of Radiolocation in CDMA Cellular Systems*, IEEE Communications Magazine, 0163-6804/98/ (April, 1998), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.1704&rep=rep1&type=pdf (last accessed: Apr. 9, 2012).

485. The primary technical standard addressing position determining services is the Telecommunications Industry Association, TIA-801-A (Revision of TIA/EIA/IS-801), *Position Determining Service for cdma2000 Spread Spectrum Systems* (Arlington, VA: Apr. 2004).

486. Aside from pilot signals, wireless carriers may employ handset-based geolocation where the wireless device uses GPS to calculate its location, which is then communicated to the nearest cell site. "By itself, GPS can be the most accurate (when satellites are acquired/available), but this technology is often enhanced by the network. Assisted GPS (AGPS) refers to a PDE system that makes use of additional network equipment that is deployed to help acquire the mobile device (much faster than non-assisted GPS) and provide positioning when the A-GPS system is unsuccessful in acquiring any/enough satellites." MobileIN.com [website], *Mobile Positioning*, 2001-2004, http://www.mobilein.com/mobile_positioning.htm (last accessed: Jul. 20, 2011).

meters for 95 percent of calls[.]"[487][488] However, E911 requirements set a minimum standard and network-based geolocation techniques have the potential to be much more accurate and intrusive. For example, TruePosition boasts that its U-TDOA network-based geolocation product "[l]ocates mobile phones and devices in any environment (indoors, in-vehicle, urban, suburban, rural, *etc.*)... with very high accuracy (typically under 50 meters)..."[489] "Described discretely, TruePosition location security solutions allow for automatic notifications based on desired criteria, such as the geographic zone of activity, specific communications patterns or particular users.... U-TDOA technology allows for locating multiple devices in real time with high accuracy. The information obtained can be viewed in a map-based format, also in real time. It includes alerting capability with regard to specific geographic areas and users."[490]

E. Global Positioning System (GPS).

Global Positioning System (GPS) "is a space-based positioning, navigation and timing system developed by the U.S. Department of Defense (DoD).... The U.S. Air Force currently finances and operates the basic system of 24+ satellites and associated ground monitoring stations located around the world. GPS is widely characterized as a satellite navigation or a satellite positioning system, providing signals for geolocation and for safe and efficient movement, measurement, and tracking of people, vehicles, and other objects anywhere from

487. 47 C.F.R. § 20.18(h)(1) *et seq.* (2008).

488. In contrast, handset-based geolocation techniques are high enough resolution if they are accurate to "50 meters for 67 percent of calls, [and] 150 meters for 95 percent of calls." *Id.*

489. *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 2nd sess. (Jun. 24, 2010) (Prepared Statement of Michael Amarosa), p. 39 (PDF, p. 43).

490. *Id.*, p. 44 (PDF, p. 48).

the earth's surface to geosynchronous orbit in space. A less-known element omitted from many GPS descriptions is the embedded timing that serves an essential role in its navigation services."[491][492] "A GPS receiver calculates its position by timing the signals sent by the GPS satellites. Each satellite continually transmits messages containing the time the message was sent, precise orbital information (the ephemeris), and the general system health and rough orbits of all GPS satellites (the almanac). The receiver measures the transit time of each message and computes the distance to each satellite. Geometric trilateration is used to combine these distances with the location of the satellites to determine the receiver's location."[493][494]

"GPS satellites provide service to civilian and military users."[495] The civilian service is

491. United States department of Defense, Defense Science Board Task Force, *The Future of the Global Positioning System* (Washington, D.C.: Oct. 2005), *available at* http://www.acq.osd.mil/dsb/reports/ADA443573.pdf (last accessed: Apr. 10, 2012), p. 25 (PDF, p. 33).

492. *See also* USDOD, *Global Positioning System Standard Positioning Service Performance Standard* (4th ed. 2008), p. 1 ("GPS has provided positioning, navigation, and timing services to military and civilian users on a continuous worldwide basis since first launch in 1978. An unlimited number of users with a civil or military GPS receiver can determine accurate time and location, in any weather, day or night, anywhere in the world.").

493. Ullah, Zafa and Goodrich, Floyd, Arrow Electronics [white paper], *GPS Technology: Know Where You Are, Know How It Works*, *available at* http://www.arrownac.com/services-tools/design/whitepapers/resource_aug09_gps.pdf (last accessed: Apr. 10, 2012), p. 2 (PDF, p. 2).

494. Location information is displayed to the user of the receiver as latitude and longitude values. *See* nationalatlas.gov, *Latitude and Longitude*, http://www.nationalatlas.gov/articles/mapping/a_latlong.html (last accessed: Aug. 30, 2011).

495. gps.gov [website], *GPS.gov: GPS Overview*, "GPS Services," *available at* http://www.gps.gov/systems/gps/ (last accessed: Apr. 24, 2012).

called the Standard Positioning Service (SPS)[496] and the military service is called the Precise Positioning Service (PPS).[497] "The civilian service is freely available to all users on a continuous, worldwide basis. The military service is available to U.S. and allied armed forces as well as approved Government agencies."[498] "Real-world data collected by the FAA show that some high-quality GPS SPS receivers currently provide better than 3 meter horizontal accuracy."[499] Because PPS broadcasts on two frequencies as apposed to the one frequency broadcast by SPS, "military users can perform ionospheric correction, a technique that reduces radio degradation caused by the Earth's atmosphere. With less degradation, PPS provides better accuracy than the basic SPS."[500] For additional information on GPS, *see Brief of Center For Democracy & Technology, Electronic Frontier Foundation, Matt Blaze, Andrew J. Blumberg, Roger L. Easton, and Norman M. Sadeh as Amici Curiae in Support of Respondent*, p. 7-14, United States v. Jones, 556 U.S. ___, 181 L. Ed. 2d 911, No. 10-1259 (2012).

---

496. "**Standard Positioning Service (SPS).** The GPS broadcast signals based on the L1 C/A-codes, as defined in IS-GPS-200, providing constellation performance to peaceful civil, commercial, and scientific users, as established in the SPS Performance Standard (SPS PS), in accordance with U.S. Government (USG) policy." USDOD, *Global Positioning System Standard Positioning Service Performance Standard*, APPENDIX C, p. C-4.

497. "**Precise Positioning Service (PPS).** The GPS broadcast signals based on the L1 P(Y)-codes, L1 C/A-codes, and L2 P(Y)-codes, as defined in the GPS ISs/ICDs, providing constellation performance to authorized users, as established in the PPS Performance Standard (PPS PS), in accordance with U.S. Government (USG) policy." *Id.*, APPENDIX C, p. C-3.

498. gps.gov [website], *GPS.gov: GPS Overview*, "GPS Services," *available at* http://www.gps.gov/systems/gps/ (last accessed: Apr. 24, 2012).

499. gps.gov [website], *GPS.gov: GPS Accuracy*, "GPS Accuracy," *available at* http://www.gps.gov/systems/gps/performance/accuracy/ (last accessed: Apr. 24, 2012).

500. *Id.*, "Is Military GPS More Accurate Than Civilian GPS".

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

F. Explanation of the term "mobile tracking device."

Mobile tracking devices are surveillance devices that can be attached to a person or object sought to be tracked. A federal statute titled "Mobile tracking devices," 18 U.S.C. § 3117, defines the broader term "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[501] Although the statutory definition of "tracking device" is not particularized, an analysis of the historical origins of 18 U.S.C. § 3117, enacted in 1986 as part of the Electronic Communications Privacy Act (ECPA), makes clear that legislators understood the term "tracking device" to mean a homing device "which might be placed in an automobile, on a person, or in some other item."[502] Prior to the wide scale use of GPS, mobile tracking devices were "beepers" or "bird dogs" consisting of "a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."[503] The beepers of the 1980s were physically installed by law enforcement in order to track a person or object for the purpose of aiding in visual surveillance.[504] Modern day mobile tracking devices still require physical installation but the tracking is now done through use of GPS satellites. For example, the Daviscomms EaziTRAC 1000 GSM/GPRS/GPS Mobile Tracking Device uses GPS satellites to generate geolocation data that

501. 18 U.S.C. § 3117(b).

502. S. Rep. No. 541, 99th Cong., 2d Sess. 10 (1986), reprinted in 1986 U.S. Code. Cong. & Admin. News 3555, 3564 (1986 Senate Report on the ECPA including a glossary of technological terms).

503. United States v. Knotts, 460 U.S. 276, 277 (1983) (beeper installed in a can of chloroform and used to track movement of car).

504. *See id.* (beeper installed in a can of chloroform and used to track movement of car); United States v. Karo, 468 U.S. 705 (1984) (beeper installed in a can of ether and tracked into residences).

can be stored and transmitted back to law enforcement via SMS messages.[505] Likewise, numerous other modern day mobile tracking devices are of similar design and function.[506]

G. Air interface surveillance equipment with an emphasis on geolocation of wireless devices.

Portable/transportable wireless device locators, virtual base stations, cell site emulators/simulators, and IMSI catchers are all generic names[507] used for hardware based surveillance equipment targeted at wireless devices such as cell phones, tablets, aircards, and other devices that communicate via a cellular air interface standard, *e.g.*, GSM, UMTS, 1xRTT, 1xEV-DO, *etc*. The surveillance devices discussed in this section operate independent from any wireless carrier network by automatically sending and/or receiving radio signals to/from target wireless devices over the air interface. Recording or "catching" IMSIs, ESNs or other identifying data; emulating base stations; locating/tracking wireless devices; conducting denial of service attacks; downloading data from wireless devices; and intercepting communications

505. *See* Daviscomms [datasheet], *GSM/GPRS/GPS Mobile Tracking Device: EaziTRAC 1000*, *available at* http://www.daviscommsusa.com/pdf/EaziTRAC%201000_Brochure_RevE1.pdf (last accessed: Jan. 5, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 035 of *2nd Consolidated Exhibits* (Dkt. #821-2) (datasheet attached).

506. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 036 of *2nd Consolidated Exhibits* (Dkt. #821-2) (collection of various web pages from http://www.alibaba.com advertising GPS based mobile tracking devices).

507. Generic names used by law enforcement for cell site emulators/simulators are "digital analyzer, cell site locator, triggerfish, ESN reader, or swamp box[.]" USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf (last accessed: Jan. 11, 2011), p. 18 of 42; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 021 of *2nd Consolidated Exhibits* (Dkt. #821-1) (relevant pages of cellfoia_release_074130_20080812.pdf attached with page numbers added).

(either passively or through a man-in-the-middle attack) are all possible functions of the type of surveillance equipment addressed in this section. While specific features vary across manufacturers, surveillance equipment targeted at wireless devices can be classified into one or both of the following general categories: (1) communication interception capabilities, and/or (2) wireless device locating/tracking capabilities. Additionally, each make/model of air interface surveillance equipment is either man-portable (using handheld controls) or vehicle-transportable (using laptop controls).[508] While a cursory glance shows that there are many similar types of off-the-shelf air interface surveillance equipment having geolocation capabilities, a more detailed analysis reveals that the RayFish line by Harris Corporation[509] is set apart from all other equipment sold by other companies. As an initial matter, Harris' RayFish product line[510] is within a class of cell site emulator capable surveillance devices—

508. In theory, either configuration would also allow for stationary operation.

509. "Harris is an international communications and information technology company serving government and commercial markets in more than 150 countries. Headquartered in Melbourne, Florida, the company has approximately $5 billion of annual revenue and more than 16,000 employees — including nearly 7,000 engineers and scientists. Harris is dedicated to developing best-in-class assured communications products, systems, and services." Harris [website], *Harris Corporation - Media Center*, http://www.harris.com/corporate-profile.html (last accessed: Sept. 28, 2010).

510. *See* [Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf, (last accessed: Mar. 9, 2011), p. 1 (StingRay does not intercept communications); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached)]; [Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last accessed: Mar. 9, 2011), p. 2 (KingFish does not intercept communications); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 007 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached)]. Product descriptions contained in Harris' StingRay and KingFish trademark documents also do not contain communications interception

which also includes devices sold by Altron,[511] NeoSoft,[512] and MMI[513]—that are specifically designed to **not** have integrated communications interception (*i.e.*, man-in-the-middle attack) capabilities. In contrast, all cell site emulator capable devices sold by Ability,[514] Meganet,[515] Shoghi Communications Ltd.,[516] Verint,[517] and View Systems[518] have integrated communications interception capabilities in addition to wireless device locating/tracking

---

capabilities. *See* [United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay registered by Harris] (registered Sep. 9, 2003), **Harris StingRay Product Description**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 10 of 88 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 005 of *2nd Consolidated Exhibits* (Dkt. #821-1) (product description attached)]; [United States Patent and Trademark Office, Trademark Reg. No. 2,867,227 [KingFish registered by Harris] (registered Jul. 27, 2004), **Harris KingFish Product Description**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 10 of 67 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 009 of *2nd Consolidated Exhibits* (Dkt. #821-1) (product description attached)].

511. *See* Altron, *GSM/UMTS Grabber: Deploying local mobile networks and secret grabbing of identification information in GSM and UMTS bands*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/87_ALTRON-GRABBER.pdf (last accessed: Apr. 10, 2012) (device does not intercept communications); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 022 of *2nd Consolidated Exhibits* (Dkt. #821-1) (PDF attached).

512. *See* NeoSoft [website], *Portable IMSI/IMEI GSM catcher NS-17-1*, http://www.neosoft.ch/products/emerg_tracking/detail.php?ID=1017&IBLOCK_ID=39 (last accessed: Feb. 10, 2012) (device does not intercept communications); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 023 of *2nd Consolidated Exhibits* (Dkt. #821-1) (print-out attached).

513. MMI sells its devices through partner companies such as Elaman and Cobham. *See* [MMI Research Trading as Cobham Surveillance, *Tactical Lawful Intercept*, PDF presentation provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/43_200906-ISS-PRG-COBHAM.pdf (last accessed: Apr. 5, 2012) (device does not intercept communications); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 024 of *2nd Consolidated Exhibits* (Dkt. #821-1) (PDF

capabilities. Regardless of whether only geolocation or geolocation with communications interception is supported, the Harris RayFish product line is entirely distinguished from all other similar products considering it offers the only cell site emulator capable air interface surveillance equipment supporting cdma2000 based air interface standards.[519] "The Harris RayFish product line includes the StingRay II, StingRay, and KingFish systems, which are

attached).]; *see also* [[Elaman, *Active Off-Air System 3GN UMTS*, Product Brochure, *available at* http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [Active Off-Air System 3GN UMTS Technical Specification.pdf] (device does not intercept communications); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 025 of *2nd Consolidated Exhibits* (Dkt. #821-1) (product brochure attached)]; [Elaman, *GSM Vehicle Direction Finder (VDF)*, Product Brochure, *available at* http://wikileaks.org/spyfiles/files/0/124_ELAMAN-200805-CATALOGUE-P1.zip (last accessed: May 14, 2012) [GSM Vehicle Direction Finder-VDF.pdf] (device does not intercept communications); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 026 of *2nd Consolidated Exhibits* (Dkt. #821-1) (product brochure attached)]].

514. *See* Ability, *3G Interception & Advanced GSM Active Solution*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/80_ABILITY-GSM_3G_Intercept.pdf (last accessed: Apr. 10, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 027 of *2nd Consolidated Exhibits* (Dkt. #821-1) (PDF attached).

515. *See* Meganet [website], *Meganet Corporation - VME Undetectable Cell Phone Interceptors*, http://www.meganet.com/meganet-products-cellphoneinterceptors.html (last accessed: Nov. 20, 2011); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 028 of *2nd Consolidated Exhibits* (Dkt. #821-2) (print-out attached).

516. *See* Shoghi Communications Ltd., *Semi Active GSM Monitoring System*, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/160_SHOGI-2006-semiactive_gsm_monitoring.pdf (last accessed: Apr. 10, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 029 of *2nd Consolidated Exhibits* (Dkt. #821-2) (PDF attached).

517. *See* Verint, *ENGAGE GI2 Models*, Product Brochure, *available at* http://files.cloudprivacy.net.s3.amazonaws.com/wikileaks-verint-location-tracking.pdf (last accessed: Apr. 5, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz.,

compatible with the **CDMA2000**, GSM, and iDEN (Nextel) protocols."[520][521][522] In contrast, all other off-the-shelf air interface surveillance equipment having geolocation through cell site emulation capabilities are limited to locating **only** GSM/UMTS[523] based wireless devices and lack compatibility with cdma2000 based wireless devices (*i.e.*, devices that operate via 1xRTT,

EXHIBIT 030 of *2nd Consolidated Exhibits* (Dkt. #821-2) (product brochure attached).

518. *See* View Systems, *Cell Phone Intercept Apparatus*, Product Brochure, *available at* http://www.viewsystems.com/pdf/CIA_11_20_06.pdf (last accessed: Apr. 5, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 031 of *2nd Consolidated Exhibits* (Dkt. #821-2) (product brochure attached).

519. The only other off-the-shelf air interface surveillance equipment compatible with cdma2000 based wireless devices operate passively (*i.e.*, no cell site emulator capabilities) and is limited to communications interception (*i.e.*, no geolocation capabilities). *See* [Stratign, *Strategic Defense Technologies*, 2011 Product Catalog, PDF provided at ISS World Europe 2008, *available at* http://wikileaks.org/spyfiles/files/0/278_STRATIGN-Catalogue-2011.pdf (last accessed: Apr. 10, 2012), p. 19; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 032 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of PDF attached)]; [Ability [website], *Passive CDMA Interceptor, ACIS – Advanced CDMA Interception System*, http://www.interceptors.com/intercept-solutions/Passive-CDMA-Interceptor.html (last accessed: May 6, 2012) ("The ACIS CDMA INTERCEPTOR is a passive monitoring system that intercepts voice and SMS traffic in cellular CDMA networks."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 033 of *2nd Consolidated Exhibits* (Dkt. #821-2) (print-out attached)].

520. Durham, NC, USA - City Council Agenda No. 7503, **Harris Sole Source Vendor Letter** (Sept. 29, 2010), *available at* http://www.durhamnc.gov/agendas/2010/cws20110103/251951_7503_342363.pdf (last accessed: Mar. 9, 2011); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 015 of *2nd Consolidated Exhibits* (Dkt. #821-1) (letter attached).

521. The Harris RayFish product line (*e.g.*, the StingRay and KingFish) also supports the 3G GSM upgrade referred to as UMTS. *See* Miami, FL, USA – Legislative Files, **Harris Sole Source Letter** (Aug. 25, 2008), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/40003.pdf (last accessed: Mar. 9, 2011), p. 2 ("The Harris StingRay and KingFish systems are compatible with the... UMTS standard..."");

1xEV-DO Rel. 0, *etc.*).[524]

1. Detailed description of the Harris RayFish line of portable/transportable wireless device locators, *i.e.*, the StingRay, KingFish, and related equipment.

Harris has been manufacturing wireless deice locators for law enforcement use since the early 1990s.[525] In February of 2009, one FBI agent testified that he alone used such

see also United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 017 of *2nd Consolidated Exhibits* (Dkt. #821-1) (letter attached).

522. Harris is also one of the few companies selling both portable *and* transportable air interface surveillance equipment that operate cooperatively. "The Harris StingRay and KingFish systems are the only cooperative portable/man-portable standard +12VDC powered/battery powered multiprotocol surveillance systems currently available." *Id*.

523. Although UMTS (the 3G upgrade for GSM) is based on W-CDMA, it is incompatible with the protocols used by cdma2000. *See* Dornan, Andy, *The Essential Guide to Wireless Communications Applications*, 2nd ed. (Prentice Hall, May 16, 2002) p. 113-14 ("Until mid-2000, the upgrade path for cdmaOne seemed clear. The end result was supposed to be a system named cdma2000 3XMC, so called because it combines three channels together, resulting in a wider band. Unfortunately, this system was not compatible with the form of W-CDMA favored by Europe and Japan, though its specifications are almost identical. The difference is the chip rate, the frequency at which the transceiver resonates. cdma2000's chip rate needs to be a multiple of cdmaOne's, while W-CDMA's has to fit the GSM framing structure.").

524. Other than for equipment sold by Harris, all cell site emulator capable air interface surveillance equipment sold by the companies discussed in this section (*i.e.*, Altron, NeoSoft, MMI, Ability, Meganet, Shoghi Communications Ltd., Verint, and View Systems) lack the ability to locate cdma2000 based wireless devices (*e.g.*,1xEV-DO Rel. 0 based aircards). *See* air interface surveillance equipment exhibits referenced in various footnotes immediately above.

525. *See* Shimomura, Tsutomu, *Catching Kevin* [Mitnick], 1993-2004 The Condé Nast Publications Inc., *available at* http://www.wired.com/wired/archive/4.02/catching_pr.html (last accessed: Apr. 5, 2012) ("The team talked to me a little about the technology they had toted along in the station wagon, especially something called a cell-site simulator, which was packed in a large travel case. The simulator was a technician's device normally used for testing cell phones, but it could also be used to page Mitnick's cell phone without ringing it, as long as he had the phone turned on but not in use. The phone would then act as a transmitter that they

equipment more than 300 times over the last nine years and that "other agencies, U.S. Marshals, Secret Service, any different number of agencies all over the country [use the equipment] every day."[526] Current era Harris products include the StingRay and KingFish as part of the RayFish line of wireless device locators. The StingRay[527] is a vehicle-transportable (*e.g.*, operational from an automobile, helicopter, airplane, *etc.*)[528][529] wireless device locator

could home in on with a Triggerfish cellular radio direction-finding system that they were using."). The TriggerFish is a first generation wireless device locator manufactured and sold by Harris. *See* United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [TriggerFish registered by Harris] (registered Jan. 29, 2002), *all associated documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed Mar. 11, 2011) (documents showing that the TriggerFish "was first used in connection with the goods at least as early as November 26, 1997...").

526. *See* United States v. Allums, No. 2:08-CR-30 TS, District of Utah (Doc. #128, p. 16 and 43) (transcripts of testimony given by FBI Agent William Shute).

527. *See* United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay registered by Harris] (registered Sep. 9, 2003), **Harris StingRay Product Pictures**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 9 & 15 of 88 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 002 of *2nd Consolidated Exhibits* (Dkt. #821-1) (pictures attached).

528. Miami, FL, USA – Legislative Files, **Harris GCSD Price List** (Sep. 2008) (Nov. 29, 2006), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/48000.pdf (last accessed: Mar. 9, 2011), p. 4 (price list having a StingRay accessory named "Airborne DF Kit CONUS" ($9,000), indicating that the StingRay may be used via helicopter, airplane, *etc.*); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 014 of *2nd Consolidated Exhibits* (Dkt. #821-1) (price list attached).

529. *See* Durham, NC, USA - City Council Agenda No. 7503, **Harris Sole Source Vendor Letter** (Sept. 29, 2010) ("When interfaced with the optional Harris AmberJack DF antenna, supported mapping software, **laptop PC controller**, and the Harris 25-Watt power amplifier kit, the StingRay can perform **vehicular-based operations**." (emphasis added)); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 015 of *2nd Consolidated Exhibits* (Dkt. #821-1) (letter attached).

with laptop location determining processor[530] and the KingFish[531] is a man-portable[532] wireless device locator with handheld PDA location determining processor.[533] As explained above, the Harris RayFish product line is able to conduct surveillance on wireless devices compatible with the cdma2000, GSM, UMTS and iDEN wireless network communication technologies.[534] The Harris "StingRay and KingFish support 3 technologies simultaneously, additional technologies can be swapped through a hardware flash process (software

530. *See id*.

531. *See* United States Patent and Trademark Office, Trademark Reg. No. 2,867,227 [KingFish registered by Harris] (registered Jul. 27, 2004), **Harris KingFish Product Picture**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 7 of 67 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 006 of *2nd Consolidated Exhibits* (Dkt. #821-1) (picture attached).

532. *See* Miami, FL, USA – Legislative Files, **Harris Sole Source Vendor Letter** (Nov. 29, 2006), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34768.pdf (last accessed: Mar. 9, 2011), p. 1 ("The **man-portability** and battery power features of the Harris KingFish product are unique for tactical mission needs, allowing the user to perform passive collection, active interrogation and active location **while on foot** (*i.e.*, inside a multi-story building, or outside in rough terrain)." (emphasis added)); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 016 of *2nd Consolidated Exhibits* (Dkt. #821-1) (letter attached).

533. *See* Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, p. 2 ("Wireless remote control from commercially available **Pocket PC**" (emphasis added)); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 007 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

534. Additionally, "[s]oftware reconfigurable architecture will allow for future software upgrades to support other wireless standards and capabilities[.]" *See* United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay registered by Harris] (registered Sep. 9, 2003), **Harris StingRay Product Datasheet**, *all associated trademark documents available via search at* http://tmportal.uspto.gov/external/portal/tow (last accessed: Mar. 11, 2011), p. 60-61 of 88 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 004 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

provided)."[535] Engineers employed by Harris explain the technology incorporated into the StingRay and KingFish as follows:

> [T]he wireless device locator may include at least one antenna and a transceiver connected thereto, and a controller for cooperating with the transceiver for transmitting a plurality of location finding signals to a target wireless communications device from among the plurality thereof. The target device may transmit a respective reply signal for each of the location finding signals.
>
> Billhartz, Thomas J., *et al.*, Harris Corp., *Wireless Communications System Including A Wireless Device Locator And Related Methods*, U.S. Patent No. 7,321,777 (Melbourne, FL: Jan. 22, 2008), *available at* http://www.freepatentsonline.com/7321777.html (last accessed: Feb. 16, 2011), p. 2, ln. 47-55.
>
> The location determining system may also include a location determining processor coupled to the receiver to collect, during movement relative to the wireless transmitter, a series of range measurements [(using propagation delays)] and a corresponding series of received signal measurements, and to estimate a location of the wireless transmitter based upon the range measurements weighted using the received signal measurements.
>
> McPherson, Rodney and Lanza, David J., Harris Corp., *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956 (Melbourne, FL: Sept. 22, 2009), *available at* http://www.freepatentsonline.com/7592956.html (last accessed: Feb. 22, 2011), p. 2, ln. 16-22.
>
> In certain embodiments, the antenna may comprise a directional antenna. In these embodiments, the location determining processor may cooperate with the directional antenna to collect, during movement relative to the wireless transmitter, a corresponding series of angle of arrival measurements. The location determining processor may also estimate the location of the wireless transmitter further based upon the angle of arrival measurements.
>
> *Id.*, p. 2, ln. 40-47.

535. Maricopa County, FL, USA – **Harris Contract**, Serial No. 09041-SS (May 27, 2010), *available at* http://www.maricopa.gov/materials/Awarded_Contracts/PDF/09041-c.pdf (last accessed: Mar. 9, 2011), p. 14; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 018 of *2nd Consolidated Exhibits* (Dkt. #821-1) (contract attached).

> Moreover, the location determining processor may cooperate with the receiver to collect, during movement relative to the wireless transmitter, a corresponding series of received signal strength measurements. The location determining processor may further estimate the location of the wireless transmitter further based upon the received signal strength measurements weighted using the received signal measurements.
>
> *Id.*, p. 2, ln. 52-58.

A Harris wireless device locator records and stores geolocation data and then uses the video display of its location determining processor (*e.g.*, laptop or PDA screen) to superimpose over a digital map the estimated location of the target wireless device.[536][537][538] McPherson and Lanza further explain that Harris wireless device locators include a GPS receiver as a platform position determining system which provides the wireless device locator with a current

536. *See* Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, p. 2 ("Provides **real-time display** of Interrogation and Passive Collection results" (emphasis added)); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 007 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

537. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last accessed: Mar. 9, 2011), p. 1 ("Optional **geolocation software** overlays target tracks and tracking vehicle location on a **digital map**"); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

538. *See* Miami, FL, USA – Legislative Files, **Harris Geolocation Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf (last accessed: Mar. 9, 2011), p. 1 ("Geolocation provides a user-friendly, geospatially accurate **mapping routine which shows on-screen** the exact location of the tracking vehicle, plus Direction of Arrival (DOA) information and/or estimated range/location information on the targeted phone.... **Tracking missions can be stored for post-mission analysis**" (emphasis added)); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 009 of *2nd Consolidated Exhibits* (Dkt. #821-1) (Geolocation Product datasheet attached).

geographical location of the platform.[539][540] The GPS receiver cooperates with the location determining processor so that the target wireless device may be located with longitude, latitude, and elevation coordinates tethered to the accuracy of the GPS coordinates of the platform.[541] When GPS signals are not available, such as when using the handheld KingFish within a building, the location determining processor may also provide for a proximity indicator involving a 3D graphic display of an arrow pointing along the azimuth and elevation angles in the direction of the target wireless device with a distance value designating the distance from the wireless device locator to the target wireless device.

Public information regarding Harris wireless device locators indicates that the Harris products allow for locating wireless devices inside buildings[542] with precision accurate to a

539. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 6, ln. 28-33.

540. The term "platform" refers to the person or vehicle transporting the wireless device locator. *See id.*, p. 3, ln. 50-54 ("The location determining system is illustratively carried by a platform movable relative to the wireless transmitter. The platform may comprise an airborne platform, for example, an aircraft, or alternatively a ground based platform, for example, an automobile." (claim notes omitted)).

541. *See id.*, p. 6, ln. 33-41.

542. *See* Miami, FL, USA – Legislative Files, **Harris Sole Source Vendor Letter** (Nov. 29, 2006) (the Harris KingFish can be used "while on foot (*i.e.*, inside a multi-story building, or outside in rough terrain)."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 016 of *2nd Consolidated Exhibits* (Dkt. #821-1) (letter attached).

singe room.[543][544] In order to achieve such a high precision, the StingRay and KingFish wireless device locators combine numerous geolocation measurement techniques to triangulate wireless devices. The geolocation techniques employed include (1) signal time-of-flight (TOF) measurements to calculate distance (a.k.a. Range), (2) signal strength measurements to calculate distance (a.k.a. range), (3) signal angle-of-arrival (AOA) measurements to calculate direction (via a phased array antenna), (4) frequency-of-arrival (FOA) measurements to calculate velocity, (5) weighting collected geolocation data and using statistical functions (*e.g.*, average, mean, median, mode, *etc.*), and (6) data fusion of calculated geolocation measurements. Whether the StingRay or KingFish, various radio signal and data collection methods are used in order to obtain signals that are subject to the noted geolocation measurement techniques. These methods include: (1) base station surveys, (2) passive interception, (3) downloading data from wireless device internal storage, (4) transmitting interrogation signals in order to force reply signals, (5) approach method for triangulation, (6) forced transmission power increase, and (7) denial-of-service attacks. The proceeding

543. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/082707_dcs01.pdf [EFF PDF Set 1 of 6] (last accessed: Oct. 25, 2010), p. 41 of 67 (The FBI indicated that it has locating equipment allowing agents "to find phones hidden in an office building and a hotel..."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

544. *See* Lapin, Lee, *How To Get Anything On Anybody – Book 3* (Mt. Shasta, CA: Intelligence Here, Jan. 15, 2003), p. 123 (Harris products are able to "track a cellular user to an area the size of a hotel room.").

subsections explain the above listed geolocation measurement techniques[545] and signal/data collection methods[546] used by the StingRay and KingFish while locating/tracking wireless devices.

a. Geolocation measurement techniques used by the StingRay and KingFish while triangulating the location of a wireless device.

i. Signal time-of-flight (TOF) measurements to calculate distance (a.k.a. range).

The StingRay uses "active... ranging techniques..."[547] in order to locate a wireless device. The StingRay's companion Geolocation software "shows on-screen the... estimated range/location information on the targeted phone."[548] A Harris patent addressing wireless device locator technology provides detailed examples of mathematical equations used in time-

545. Frequency-of-arrival (FOA) is not explained because such measurements are not relevant to the aircard locating mission in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.). For an explanation of FOA, *see*, *e.g.*, Ryu, Kil-Hyen, Samsung Electronics Co., Ltd., *Apparatus And Method For Estimating A Doppler Frequency And A Moving Velocity Of A Wireless Terminal*, U.S. Patent No. 7,529,328 (Suwon-si, KR: May 5, 2009), *available at* http://www.freepatentsonline.com/7529328.html (last accessed: Feb. 16, 2011).

546. Passive interception and denial-of-service attack via jamming are not explained because such methods are not relevant to the aircard locating mission in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.). However, the FBI conducted two other types of denial-of-service attacks that are discussed in *How The Aircard Was Intruded Upon*, *infra*.

547. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, p. 1; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

548. *See* Miami, FL, USA – Legislative Files, **Harris Geolocation Product Datasheet**, p. 1; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 009 of *2nd Consolidated Exhibits* (Dkt. #821-1) (Geolocation Product datasheet attached).

of-flight (TOF) measurements for conducting ranging techniques.[549] A wireless device locator employing TOF[550] will measures the propagation delay time of signals received from a target wireless device in order to find the distance between the wireless device locator and the target wireless device.[551] If the wireless device locator knows the transmission time of a signal,[552] it can subtract that time from the signal receive time to obtain the time-of-flight. Because all radio waves travel at the speed of light,[553] multiplying the time-of-flight by the speed of light

549. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 7 *et seq.* ("Time of Flight Based Approach").

550. TOF is also sometimes referred to as time-of-arrival (TOA). *See*, *e.g.*, Coluzzi, Michael, E. and Kang, Sung P., ITT Manufacturing Enterprises, Inc., *Method And System For Determining The Position Of An Object*, U.S. Patent No. 7,187,327 (Los Angeles, CA: Mar. 6, 2007), *available at* http://www.freepatentsonline.com/7187327.html (last accessed: Feb. 22, 2011), p. 6, ln. 6-25 (explaining TOF measurements but referring to them as TOA).

551. *See* Kim and Lee, *Apparatus And Method For Tracking Location Of Mobile Station*, U.S. Patent App. No. 2003/0117320, p. 4, ¶ 15.

552. As previously explained, for 1xEV-DO Rel. 0 cellular data networks, the Access Terminal (*i.e.*, target wireless device) and Access Network (*e.g.*, StingRay or KingFish) establish a common time reference that is used to derive timing for the transmitted chips, symbols, slots, frames, and system timing over the air interface. *See Technical Explanations*, Section III(B)(3)(f), *supra*. Because of the common timing, the Access Network always knows the time at which the Access Terminal transmits a signal. *See id*. Harris wireless device locators take advantage of the common timing reference in order to obtain a precise transmission time for CDMA based signals transmitted from a target wireless device. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 4 ln. 56-59 ("[T]he time of flight measurements may be generated using a time of transmission stamp within the reply signal by differing the reply signal receipt time with the indicated time of transmission.").

553. *See Technical Explanations*, Section III(A), *supra* (explaining electromagnetic radiation in the radio frequency band); Jandrell, Louis H. M., Pinpoint Communications, Inc., *Communication system and method for determining the location of a transponder unit*, U.S. Patent No. 5,526,357 (Dallas, TX: Jun. 11, 1996), *available at* http://www.freepatentsonline.com/5526357.html (last accessed: Feb. 16, 2011), p. 16, ln. 18-19

gives a measurement of distance from the wireless device locator to the target wireless device.[554] Knowledge of one TOF distance measurement constrains the location of the target wireless device to any point along the circumference of a circle in a 2D coordinate system, or to any point on the surface of a sphere in a 3D coordinate system—with each scenario having the wireless device locator at the center.[555] If a second propagation delay can be measured from a second known location, the result is the intersection of two circles in 2D, which in turn constrains the location of the wireless device to two intersecting points, or the result is the intersection of two spheres in 3D, which in turn constrains the location of the wireless device to any point around the circumference of a circle created by the intersecting spheres.[556] Knowledge of at least three propagation delays measured from three separate known locations will resolve the ambiguity in a 2D coordinate system and constrain the location of the wireless

("...radio signals travel at the speed of light, approximately 0.98357 ft. per nanosecond through air...").

554. *See* Hall, Christopher, J. *et al*., *Method and apparatus for geolocating a wireless communications device*, U.S. Patent No. 7,057,556 (Satellite Beach, FL: Jun. 6, 2006), *available at* http://www.freepatentsonline.com/7057556.html (last accessed: Feb. 22, 2011), p. 2, ln. 37-42

555. *See* Caffery and Stüber, *Overview of Radiolocation in CDMA Cellular Systems*, IEEE Communications Magazine, 0163-6804/98/, p. 39 (explaining TOF in a 2D coordinate system); *see also* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 7-9 (proving TOF geolocation measurement equations for a 3D coordinate system, *i.e.*, inclusion of altitude).

556. *See* Moeglein, Mark and Riley, Wyatt, Qualcomm, Inc., *Method And Apparatus For Location Determination In A Wireless Assisted Hybrid Positioning System*, U.S. Patent App. No. 2004/0002344 (Ashland, OR: Jan. 1, 2004), *available at* http://www.freepatentsonline.com/y2004/0002344.html (last accessed: Sept. 29, 2010), p. 1, ¶ 8; McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 7-9 (proving TOF geolocation measurement equations for a 3D coordinate system, *i.e.*, inclusion of altitude)

device to one of the two previously discussed intersecting points.[557] Knowledge of at least four propagation delays measured from four separate known locations will resolve the ambiguity in a 3D coordinate system and constrain the location of the target wireless device to a single point along the circumference of the previously discussed circle.[558]

ii. Signal strength measurements to calculate distance (a.k.a. range).

The StingRay "[i]nterfaces with AmberJack antenna to form a complete target tracking and location solution using active... ranging techniques..."[559] The AmberJack phased array beam-forming antenna "[d]etermines... received signal strength of a targeted mobile phone's transmission[.]"[560] Similarly, the KingFish "[d]ynamically updates received signal strength to enable precise location of a target phone[.]"[561] A Harris patent addressing wireless device locator technology provides detailed examples of mathematical equations used in power-distance measurements for conducting ranging techniques.[562] A wireless device locator having

557. *See* references cited in fn. No. 555, *supra*.

558. *See* references cited in fn. No. 556, *supra*.

559. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, p. 1; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

560. Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, p. 6-7; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 011 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

561. Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, p. 2; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 007 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

562. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 9 *et seq.* ("Received Signal Strength

a power-distance detector will measure the difference between the signal receive power and the signal transmit power in order to determine the distance between the wireless device locator and the target wireless device that transmitted the signal.[563] If the wireless device locator knows the transmit power of the signal,[564] it can subtract that value from the signal receive power to obtain the loss power value.[565] Because the intensity of radio wave propagation in free space is inversely proportional to the square of the distance traveled,[566] knowledge of the loss power value constrains the location of the target wireless device to any point around the circumference of a circle in a 2D coordinate system, or to any point on the surface of a sphere in a 3D coordinate system—with each scenario having the wireless device locator at the center.[567] The process for resolving 2D and 3D location ambiguity for a target wireless device while

Indication Based Approach").

563. *See* Kim and Lee, *Apparatus And Method For Tracking Location Of Mobile Station*, U.S. Patent App. No. 2003/0117320, p. 2, ¶ 32.

564. "[F]or signal-strength-based [geolocation measurement] systems it is necessary that the transmit power of the MSs be known and controlled with reasonable accuracy." Caffery and Stüber, *Overview of Radiolocation in CDMA Cellular Systems*, IEEE Communications Magazine, 0163-6804/98/, p. 39. As previously explained, for 1xEV-DO Rel. 0 cellular data networks, the Access Network (*e.g.*, StingRay or KingFish) controls the transmit power of the Access Terminal (*i.e.*, target wireless device) by sending it commands called Reverse Power Control (RPC) Bits. *See Technical Explanations*, Section III(B)(3)(e)(ii), *supra*. Therefore, the StingRay and KingFish while operating in cell site emulator mode have the ability to know and control the transmit power of a target wireless device.

565. *See* Proctor, James A, Jr. and Otto, James C., Harris Corp., *Range And Bearing Tracking System With Multipath Rejection*, U.S. Patent No. 5,687,196 (Indialantic, FL: Nov. 11, 1997), *available at* http://www.freepatentsonline.com/5687196.html (last accessed Feb. 16, 2011), p. 1, ln. 29-37.

566. *See id*.

567. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System*

using power-distance measurements is identical to what is used in TOF involving the intersection of multiple circles or spheres.[568] In U.S. Patent No. 7,592, 956, McPherson *et al.* of Harris provides a diagram showing three power-distance circles (only two are drawn) plotted on a 2D map intersecting where the target wireless device is located.[569] However, as indicated by the mathematical equations taught by McPherson *et al.*, the power-distance geolocation measurement technique is typically used to locate wireless devices in a 3D coordinate system, *i.e.*, the inclusion of altitude.[570]

iii. Signal angle-of-arrival (AOA) measurements to calculate direction (via a phased array antenna).

Measurements of signal angle-of-arrival (AOA) are used to obtain a 3D directional fix (azimuth angle and elevation angle) on a target wireless device having an unknown location relative to the wireless device locator.[571] The azimuth angle points in the direction of the wireless device along the horizontal plane and the elevation angle points in the direction of the

And Related Methods, U.S. Patent No. 7,592,956, p. 9, ln. 38-67; p. 10, ln. 1-67.

568. *See Technical Explanations*, Section III(G)(1)(a)(i), *supra* (explaining TOF geolocation measurements used by the StingRay and KingFish to locate wireless devices).

569. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, Figure No. 10.

570. *See id.*, p. 9, ln. 38-67; p. 10, ln. 1-67.

571. *See* Kim, Eung-Bae and Lee, Seung-Hwan, *Apparatus And Method For Tracking Location Of Mobile Station*, U.S. Patent App. No. 2003/0117320 (Daejeon, KR: Jun. 26, 2003), *available at* http://www.freepatentsonline.com/y2003/0117320.html (last accessed: Feb. 16, 2011), p. 1, ¶ 13; McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 11, ln. 9-19.

wireless device along the vertical plane.[572] "There are a myriad of methods for determining the angle of arrival of a signal at a receiving site, such as by: the use of a rotating antenna which is rotated to obtain the strongest signal from the target unit; a phase array of antenna elements which may be variably electrically steered to obtain the strongest signal; plural antennas at which the receiving unit may compare the instantaneous phase of the arriving signal at each of the plural antennas to determine the direction of a signal...; or other conventional methods."[573] The most advanced direction finding antenna is the phased array beam-forming antenna.[574] "An array antenna is a special arrangement of basic antenna components."[575] "In an array propagating a given amount of energy, more radiation takes place in certain directions than in others. The elements in the array can be altered in such a way that they change the pattern and distribute it more uniformly in all directions.... On the other hand, the elements could be arranged so that the radiation would be focused in a single

572. *See* Kim and Lee, *Apparatus And Method For Tracking Location Of Mobile Station*, U.S. Patent App. No. 2003/0117320, p. 4, ¶ 15.

573. *See* Otto, James C., Harris Corp., *System And Method For Determining The Geolocation Of A Transmitter*, U.S. Patent No. 5,719,584 (Indian Harbor Beach, FL: Feb. 17, 1998), *available at* http://www.freepatentsonline.com/5719584.html (last accessed: Feb. 22, 2011), p. 3, ln. 38-47.

574. "The signals induced on different elements of an array in space are combined to form a single output (*beam*) of the array. This process of combining the signals from different elements is known as *beam forming*. The direction at which the array has maximum response (array has maximum gain) is said to be the *beam pointing direction or look direction*." Akhter, Mohammad S., *Signal Processing for MC-CDMA*, Master of Engineering (by Research) Dissertation, The University of South Australia (Mar. 1998), p. 70.

575. United States Army, *Communications-Electronics Fundamentals: Wave Propagation, Transmission Lines, and Antennas*, p. 4.29 (PDF, p. 195).

direction."[576] Changing the directivity of a phased array antenna involves altering the phase of the antenna elements so that the various propagated radio waves either reinforce or cancel one another in controlled directions.[577] The controlled directivity of a phased array antenna is the same for receiving signals as for transmitting signals.[578][579]

Harris wireless device locators are used with the AmberJack phased array antenna with beam-forming technology.[580] "AmberJack is a phased array direction-finding (DF) antenna system capable of tracking and locating mobile phone users and base stations."[581] "AmberJack combines Harris' expertise in phased array antenna technology and tracking and locating

576. *Id.*, p.4.32 (PDF, p. 198).

577. "Various reflected and refracted components of the propagated wave create effects of reinforcement and cancellation. At certain distant points from the transmitter, some of the wave components meet in space. Reception at these points is either impaired or improved. If the different components arrive at a given point in the same phase, they add, making a stronger signal available. If they arrive out of phase, they cancel, reducing the signal strength." *Id.*, p. 4.30, (PDF, p. 196).

578. *See id.*, p. 4.11 (PDF, p. 177) ("When a transmitting antenna with a certain gain is used as a receiving antenna, it will also have the same gain for receiving.").

579. When determining a line bearing via received signals, "[t]he angle of arrival of the response signal may be determined by evaluating the phase of the response signal simultaneously at each of the antennas. The simultaneous phase relationships at the antennas, the geometric relationship of the antennas and the frequency of the response signal can be used to estimate the angle of arrival of the response signal with respect to the antennas." *See* Proctor and Otto, Harris, *Range And Bearing Tracking System With Multipath Rejection*, U.S. Patent No. 5,687,196, p. 1, ln. 47-53.

580. *See* Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/40003.pdf (last accessed: Mar. 9, 2011), p. 6-7; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 011 of *2nd Consolidated Exhibits* (Dkt. #821-1) (AmberJack datasheet attached).

581. *Id.*

systems to offer a state-of-the-art direction finding system. Beam forming technology offers a universal DF antenna for existing as well as future cellular standards."[582] The AmberJack is specifically designed to operate with the StingRay and allows it to determine "direction of arrival and received signal strength of a targeted mobile phone's transmissions."[583] "Harris' unique adaptive array processing techniques provide for automatic signal optimizing, interference suppression, and custom beam shaping."[584] For adaptive antenna arrays, "the gain and phase of individual antennas are changed before combining to adjust the overall gain of the array in a dynamic fashion as required by the system [(*i.e.*, electronically changing the direction of the beam in real-time)]."[585] Harris' phased array antennas are backed by 20+ years of experience with capabilities that "combine two separate processes, classical antenna array design and antenna array signal processing, to significantly improve signal-to-noise, geolocation accuracy and Angle of Arrival estimates."[586]

582. Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last accessed: Mar. 9, 2011), p. 2; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 010 of *2nd Consolidated Exhibits* (Dkt. #821-1) (AmberJack datasheet attached).

583. Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, p. 6-7; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 011 of *2nd Consolidated Exhibits* (Dkt. #821-1) (AmberJack datasheet attached).

584. Harris, Government Communications Systems Division, *Phased Array Antennas Brochure* (2004), *available at* http://download.harris.com/app/public_download.asp?fid=450 (last accessed: Sept. 22, 2010); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 012 of *2nd Consolidated Exhibits* (Dkt. #821-1) (Phased Array Antennas Brochure attached).

585. Akhter, *Signal Processing for MC-CDMA*, The University of South Australia, p. 69.

586. Harris, Government Communications Systems Division, *Phased Array Antennas Brochure*; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 012

iv. Weighting collected geolocation data and using statistical functions (*e.g.*, average, mean, median, mode, *etc.*).

In order to more precisely determine the location of a target wireless device, the wireless device locator will use received signal measurements to weight received signals corresponding to any given measurement family (*e.g.*, TOF, power-distance, AOA, *etc.*). Received signal measurements may consist of bit-error rate measurements, received signal strength measurements, receiver metrics, and signal-to-noise ratio measurements.[587] When the received signal measurements indicate a high quality received signal, such as when the signal-to-noise ratio value is larger, the wireless device locator interprets the other associated signal measurements (used to determine the location of the target wireless device) to be of higher quality and weights those measurements more heavily while producing the location estimate.[588] The wireless device locator may also use statistical functions (*e.g.*, mean, median, mode, *etc.*) on a group of geolocation measurements within a set of measurements corresponding to any given measurement family in order to more precisely determine the location of a target wireless device.[589] Both weighting and averaging depend on a multitude of geolocation measurements, preferably taken from different locations in order to increase the variety of the relevant signals.[590]

---

of *2nd Consolidated Exhibits* (Dkt. #821-1) (Phased Array Antennas Brochure attached).

587. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 5, ln. 57-64.

588. *See id.*, p. 5, ln. 64-67; p. 6, ln. 1-7.

589. *See* Billhartz, *et al.*, Harris, *Wireless Communications System Including A Wireless Device Locator And Related* Methods, U.S. Patent No. 7,321,777, p. 7, ln. 56-59.

590. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System*

v. Data fusion of calculated geolocation measurements.

In order to more precisely determine the location of a target wireless device, the wireless device locator will use data fusion by combining and simultaneously using the various collected geolocation measurements spanning multiple measurement families (*e.g.*, TOF, power-distance, AOA, *etc.*).[591] By using data fusion, different families of measurements, and even measurements within families, can be combined in a weighted sense to arrive at an optimized target wireless device location estimate.[592] Using data fusion across multiple measurement families increases the precision of locating a wireless device considering suspected measurement errors within any given measurement family can be given less weight or even eliminated completely.[593] For example, the propagation delay used to determine distance in a TOF measurement may be imprecise due to measurements taken on multipath signals having a longer propagation delay when compared to direct path signals. The noted measurement errors may be eliminated by fusing power-distance geolocation data with TOF geolocation data.[594] Data fusion may also be used to fill measurement voids that may be present within any given measurement family. For example, the TOF geolocation measurement technique requires at least three separate measurements in order to confine the location of a

And Related Methods, U.S. Patent No. 7,592,956, p. 6, ln. 18-27.

591. *See id.*, p. 13, ln. 50-59.

592. *See id.*, p. 14, ln. 34-39.

593. *See id*.

594. *See* Kim and Lee, *Apparatus And Method For Tracking Location Of Mobile Station*, U.S. Patent App. No. 2003/0117320, p. 3, ¶ 38.

target wireless device to a single point in a 2D coordinate system.[595] This limitation may be eliminated by fusing AOA measurements with an inadequate number of TOF measurements in order to achieve the same precision that would otherwise be achieved using an adequate number of TOF measurements.[596] Just like weighting and averaging within signal measurement families, data fusion depends on a multitude of geolocation measurements preferably taken from different locations in order to increase the variety of the relevant signals.[597]

b. Radio signal and data collection methods used by the StingRay and KingFish while triangulating the location of a wireless device.

i. Base station surveys.

Among other surveillance capabilities, the StingRay "performs network base station surveys.."[598] in any given network coverage area. Similarly, the KingFish "[i]dentifies active CDMA channels and catalogs base station parameters[.]"[599] Harris wireless device locators

595. *See Technical Explanations*, Section III(G)(1)(a)(i), *supra* (explaining TOF geolocation measurements used by the StingRay and KingFish to locate wireless devices).

596. *See* Otto, Harris, *System And Method For Determining The Geolocation Of A Transmitter*, U.S. Patent No. 5,719,584, p. 4, ln. 6-23.

597. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 6, ln. 18-27.

598. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, p. 1; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

599. Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, p. 2; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 007 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

are used with the AmberJack phased array antenna, which "[d]etermines... received signal strength of a targeted base station's transmission[.]"[600] The *Allums* court opinion, published as United States v. Allums, No. 2:08-CR-30 TS, 2009 WL 806748 (D.Utah 2009), paraphrases sworn testimony given by FBI Agent William Shute on the StingRay's base station survey capabilities:

> Shute testified that he identified the originating cell tower for each of the calls in question. Shute testified that he purchased a cell phone from the same service provider as the Defendant and placed the phone into 'engineering mode,' where the phone display showed the cell tower to which it was currently connected. Using that phone and another device called a Stingray, which also tracked which cell tower was the strongest at any geographical position, Shute drove for some time around the neighborhoods surrounding the cell towers in question and determined an approximate range for each cell tower. Specifically, Shute testified that he was able to determine the approximate distance from the originating cell tower where the cell phone and Stingray switched from the originating cell tower to another cell tower. Shute testified that this method allows him to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed.

Id. at 1.

ii. Cell site emulation and forced connection handoff.

The datasheet for the StingRay states that it "emulates base station to collect MINs and

600. Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, p. 7; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 011 of *2nd Consolidated Exhibits* (Dkt. #821-1) (AmberJack datasheet attached).

ESNs through forced registration[.]"[601][602] Lee Lapin, former government surveillance advisor, also indicated in his book that various Harris wireless device locators emulate base stations and force wireless devices to connect to the government's emulated cellular networks.[603] Lapin explained cell site emulation as "[e]mulat[ing] Base Station Control Channel to 'capture' mobile phones in close proximity[.]"[604] Documents from the Executive Office for United States Attorneys indicate that a cell site emulator "is a mobile device that can electronically force a cell phone to register its telephone number (MIN), electronic serial number (ESN), and information about its location, when the phone is turned on. This can be done without the user knowing about it, and without involving the cell phone provider."[605] While operating in cell site emulator mode, the wireless device locator will appear to all compatible wireless devices within signal range as an actual and legitimate cell site

601. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, p. 1; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

602. In the context of modern day mobile communications standards, the meaning of the term "registration" as used by Harris should be read as "forced handoff" because the handoff to the cell site emulator occurs first and whether "registration" occurs depends on the cellular technology at issue. For example, 1xRTT wireless devices "register" with the StingRay while 1xEV-DO Rel. 0 wireless devices conduct session establishment with the StingRay. *See Technical Explanations*, Section III(B)(3)(c)(iii), *supra*.

603. *See* Lapin, Lee, *How To Get Anything On Anybody – Book 3*, Intelligence Here (Mt. Shasta, CA: Jan. 15, 2003), p. 122-23.

604. *See id.*, p. 122.

605. USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, p. 18 of 42; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 021 of *2nd Consolidated Exhibits* (Dkt. #821-1) (relevant pages of cellfoia_release_074130_20080812.pdf attached with page numbers added).

indistinguishable from cell sites operated by the wireless carrier. If configured for cdma2000 technologies, the wireless device locator will broadcast a high powered pilot signal, which will force the target wireless device to disconnect from its legitimate serving cell site and connect to the emulated cell site. Once forced to connect to the emulated cell site, the wireless device locator seizes control of the wireless device allowing for interrogation, downloading of stored data, denial-of-service attacks, and other supported operations.[606] The Harris RayFish line of wireless device locators can emulate cell sites across a wide range of mobile network protocols. As previously explained, the RayFish line is compatible with cdma2000, GSM, UMTS, and iDEN protocols with a maximum of three mobile network software packages loaded at any given time.[607] In order to emulate a cell site under any given protocol, the StingRay and KingFish must follow the procedures set forth in the relevant communications standards set by international standards setting bodies.[608]

iii. Downloading data from wireless device internal storage.

The StingRay "[s]upports targeting and real-time searching of mobile identification numbers (MIN), dialed numbers, and electronic serial numbers (ESN)[.]"[609] Similarly, the

606. *See Technical Explanations*, Section III(G)(1)(b)(iii) through (vi), *infra*.

607. *See id.*, Section III(G)(1), *supra*.

608. *See*, *e.g.*, TIA-2000.1-E, *Introduction to cdma2000 Spread Spectrum Systems*, § 1.1.1, p. 1.1 ("The technical requirements contained in cdma2000 form a compatibility standard for CDMA systems. They ensure that a mobile station can obtain service in a system manufactured in accordance with the cdma2000 standards.").

609. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, p. 1; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

KingFish "provides investigators with a tool that extracts the telephone number (MIN) and Electronic Serial Number (ESN) from a CDMA mobile telephone."[610] Harris trademark documents for "StingRay" and "KingFish" also indicate that the devices are used for "gathering information from cellular telephones..."[611] The process of searching for and extracting data from a target wireless devices, as supported by the StingRay and KingFish, begins after the wireless device is forced to connect to the emulated cellular network being broadcast.[612] For example, if operating as a 1xEV-DO Rel. 0 cell site, the wireless device locator will establish a session with the target wireless device in order to transmit signals containing a HardwareIDRequest message allowing the wireless device locator to download the ESN stored within the target wireless device.[613] By downloading identifying information from each wireless device that connects to the cell site emulator, the wireless device locator determines which wireless device is the target wireless device sought to be located and which

610. Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, p. 2; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 007 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

611. *See* [United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay registered by Harris] (registered Sep. 9, 2003), **Harris StingRay Product Description**, p. 10 of 88 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 005 of *2nd Consolidated Exhibits* (Dkt. #821-1) (product description attached)]; [United States Patent and Trademark Office, Trademark Reg. No. 2,867,227 [KingFish registered by Harris] (registered Jul. 27, 2004), **Harris KingFish Product Description**, p. 11 of 67 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 008 of *2nd Consolidated Exhibits* (Dkt. #821-1) (product description attached)].

612. *See Technical Explanations*, Section III(G)(1)(b)(ii), *supra*.

613. *See id.*, Section III(B)(3)(c)(v), *supra* (explaining the 1xEV-DO Rel. 0 HardwareIDRequest and HardwareIDResponse messages).

wireless devices are to be ignore.

iv. Transmitting interrogation signals in order to force reply signals.

The StingRay datasheet contains a heading reading "Transmit Capabilities" with "For Interrogation and Active Tracking and Location" under the heading.[614] Similarly, the KingFish datasheet is titled "Portable CDMA Interrogation... System[.]"[615] The term "interrogation" in the geolocation context is adapted from radar terminology.[616] "The process by which a radar transmits a signal suitable for triggering the beacon is known as interrogation; the corresponding beacon transmission is termed the reply. Radar beacons which reply to interrogations are called transponders and the radar set used to interrogate a beacon is called an interrogator."[617] A Harris patent addressing wireless device locator technology explains that interrogation in the geolocation context involves "prompt[ing] the target wireless communications device to send reply signals using the location finding signals, rather than passively waiting until the target device begins transmitting. This allows for quicker and more

614. *See* United States Patent and Trademark Office, Trademark Reg. No. 2,762,468 [StingRay registered by Harris] (registered Sep. 9, 2003), **Harris StingRay Product Datasheet**, p. 61 of 88 page compilation; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 004 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

615. Miami, FL, USA – Legislative Files, **Harris KingFish Product Datasheet**, p. 2; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 007 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

616. Kelly, Robert J. and Cusick, Danny R., *Advances in Electronics and Electron Physics, Volume 68*, ed. Hawkes, Peter W., "Distance Measuring Equipment and Its Evolving Role in Aviation" (Orlando, FL: Academic Press, Inc., 1986), p. 7.

617. *Id*.

efficient device location."[618] Another relevant Harris patent explains that a location finding signal "may comprise a signal that would routinely prompt a transmission reply from the wireless transmitter under the applicable communications standard. Once the wireless transmitter receives the signal from the location determining system, the wireless transmitter transmits a reply signal that is received by the platform."[619] In order to force a target wireless device to generate an abundance of response signals during interrogation, the wireless device locator will exploit elements of the applicable mobile communications protocol being used by the target wireless device.[620] For example, if emulating a 1xEV-DO Rel. 0 cellular data network, the wireless device locator may force the target wireless device to transmit an abundance of ACK signals that would go unnoticed by the wireless device user.

v. Approach method for triangulation.

The StingRay utilizes "active approach" in order to triangulate the location of a target wireless device.[621] A relevant Harris patent explains that a wireless device locator engaged in

618. *See* Billhartz, *et al.*, Harris, *Wireless Communications System Including A Wireless Device Locator And Related* Methods, U.S. Patent No. 7,321,777, p. 2, ln. 67; p. 3, ln. 1-5. The Harris patent also references U.S. Patent No. 5,706,010 (bridging the technology reference gap between radar and geolocation for wireless devices).

619. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 4, ln. 43-48.

620. *See* Billhartz, *et al.*, Harris, *Wireless Communications System Including A Wireless Device Locator And Related* Methods, U.S. Patent No. 7,321,777, p. 6, ln. 29-36 ("By way of example, the location finding signal may include the UID of the target device in a header packet and a valid but empty data packet. This will force the target device to generate a reply signal acknowledging receipt of the location finding signal (*i.e.*, an ACK signal). Of course, various other location finding signals could be used to cause the target terminal to generate the ACK signal, as will be appreciated by those skilled in the art." (claim note omitted)).

621. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, p. 1; *see*

"approach" is fixed to a portable/transportable platform (*e.g.*, airplane, automobile, person, *etc.*) so that it may collect geolocation measurements during movement relative to the wireless device being located,[622] *i.e.*, while it "approaches" the wireless device. "As the platform moves relative to the wireless transmitter, the accuracy of the location estimate improves if the trajectory of the platform: breaks symmetry with regards to the wireless transmitter, reduces ambiguity resolution, and minimizes geometric dilution of precision (GDOP)."[623] The Harris patent further explains that "it may be preferable to encircle the approximate location of the wireless transmitter to provide more accurate results, *i.e.*, breaking the symmetry."[624] In referencing this method, the USDOJ Electronic Surveillance Manual states that "[l]aw enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones[, and b]y shifting the location of the device, the operator can determine the phone's location more precisely using triangulation."[625] The approach method is the primary

also United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

622. *See* McPherson and Lanza, Harris, *Wireless Transmitter Location Determining System And Related Methods*, U.S. Patent No. 7,592,956, p. 3 ln. 48-57.

623. *Id.*, p. 6 ln. 13-17 (claim note omitted).

624. *Id.*, p. 6 ln. 50-53 (claim note omitted). In providing further explanation, McPherson *et al.* also makes reference to Figure No. 8, attached to the cited patent, showing a wireless device locator aboard an airplane taking three different range bearing measurements from three different positions in order to triangulate the location of a cellular phone. *See also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 52 of *1st Consolidated Exhibits* (Dkt. #587-1) (Figure No. 8, attached).

625. U.S. Dep't of Justice, *Electronic Surveillance Manual*, p. 45 (emphasis added). *See also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 052 of *2nd Consolidated Exhibits* (Dkt. #821-3) (section on cell site emulators, *etc.*, p. 40-41 and 44-45).

benefit of using a portable/transportable wireless device locator, as apposed to a stationary wireless device locator (*e.g.*, a cell site with location finding hardware and software), because it allows for many geolocation measurements to be taken from different locations within a short time period. For example, if being transported in an automobile while in cell site emulator mode, a wireless device locator may take a geolocation measurement from a different location once every three seconds.[626] Therefore, if the wireless device locator is transported within the area of the target wireless device over the course of 30 minutes, it would be the equivalent of having 600 wireless carrier cell sites working together to triangulate the location of the target wireless device.

vi. Forced transmission power increase.

Increasing the signal transmission power of a target wireless device is standard functionality for all wireless device locators. The Wiki for the OsmocomBB based "IMSI Catcher Catcher" software—designed to detect and defeat wireless device locators such as the StingRay and KingFish—lists "[y]our phone sends at the highest possible power"[627] as one of the StingRay/KingFish detection mechanisms. The process of instructing a target wireless device to transmit at the highest possible power, as supported by the StingRay and KingFish, is

626. *See* Billhartz, *et al.*, Harris, *Wireless Communications System Including A Wireless Device Locator And Related* Methods, U.S. Patent No. 7,321,777, p. 8, ln. 63-64 ("Preferably, the location finding signals are transmitted over a relatively short interval (a few seconds or less)...").

627. srlabs.de [website], *Catcher Catcher - Wiki – Redmine*, *available at* http://opensource.srlabs.de/projects/catcher/wiki/Wiki (last accessed: Apr. 5, 2012); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 034 of *2nd Consolidated Exhibits* (Dkt. #821-2) (Wiki page attached).

done after the wireless device is forced to connect to an emulated cellular network.[628] Once the target wireless device is connected to the emulated cellular network, the wireless device locator employs closed-loop power control[629][630] while transmitting signals instructing the target wireless device to transmit at the highest possible power. For example, if locating a 1xEV-DO Rel. 0 wireless device, the wireless device locator will transmit Reverse Power Control (RPC) bits, with a value of "1,"[631] to the target wireless device until it is transmitting at the highest possible power. By increasing the transmit power of the target wireless device, the wireless device locator is able to collect higher quality signals sent in response to the location finding interrogation signals.[632] By collecting higher quality response signals, geolocation measurements become more accurate and the precision of the location estimate increases.

H. The FBI Digital Collection Program.

The FBI Digital Collection Program provides agents "with the means to collect evidence and intelligence through the acquisition, deployment, and support of communications

628. *See Technical Explanations*, Section III(G)(1)(b)(ii), *supra*.

629. "[I]n CDMA cellular systems the MSs are power controlled to combat the near-far effect. Time-division multiple access (TDMA) cellular systems use power control to conserve battery power in the Mss." *See* Caffery and Stüber, *Overview of Radiolocation in CDMA Cellular Systems*, IEEE Communications Magazine, 0163-6804/98/, p. 39.

630. *See Technical Explanations*, Section III(B)(3)(e)(ii), *supra* (explaining 1xEV-DO Rel. 0 closed-loop power control on the Reverse Traffic Channel).

631. *See Technical Explanations*, Section III(B)(3)(e)(ii).

632. *See id.*, Section III(G)(1)(b)(iv), *supra* (explaining interrogation used by the StingRay and KingFish to locate wireless devices).

interception techniques and systems which facilitate and support national security, domestic counterterrorism, and criminal investigative efforts."[633] In more practical terms, the FBI Digital Collection Program provides agents of the FBI a means to: (1) collect communications content, (2) collect signaling information (*i.e.*, Pen/Trap data)[634] relating to transmitted communications, and (3) geolocate wireless devices such as cell phones and aircards. The Digital Collection Program is comprised of numerous elements including: (1) computer hardware and software, (2) surveillance equipment, (3) a specialized network used for intercepting data directly from telecommunications providers, (4) technical standards, (5) data collection and delivery points, (6) designated personnel responsible for administrating and operating the program, and (7) FBI policy dictating operations of the program. The proceeding subsections provide a brief explanation of various elements making up the FBI Digital Collection Program, as explained in FBI documents.

1. Digital Collection Systems.

In order to receive data collected through the Digital Collection Program, agents use specialized computers, referred to as Digital Collection Systems, comprised primarily of

633. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071217_dcs05.pdf [EFF PDF Set 5 of 5] (last accessed: Oct. 25, 2010), p. 33 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

634. The term "Pen/Trap data" is shorthand for any data that may be obtained via a pen register and/or trap and trace device as defined in 18 U.S.C. §§ 3127(3) (pen registers) and 3127(4) (trap and trace devices).

commercial-off-the-shelf hardware and software with limited proprietary application software.[635] The FBI began development of Digital Collection Systems in late 1996.[636] These systems intercept multi-source digital (and analog) communications information for intelligence gathering applicable to foreign counterintelligence activities and for investigative purposes for providing evidence at criminal trials.[637] The electronic information collected includes Pen/Trap data (*i.e.*, call-identifying information), analog and digital call content, facsimile transmissions, modem transmissions, microphone audio,[638] real-time cell site location information,[639] and other real-time geolocation information. Digital Collection Systems process and evaluate the collected electronic information "for migration to a separate information technology system where the collected data is analyzed, managed and archived as case related information. Processing of information collected through digital collection

635. *See id*.

636. *See* FBI Jul. 2, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/070207_dcs08.pdf [EFF PDF Set 8 of 8] (last accessed: Oct. 25, 2010), p. 37 ("In late 1996, TICTU spearheaded the development of a unique telecommunications access program called 'DCS-3000,' a system capable of interfacing with the switching facilities of many wireless carriers that deploy new digital technologies..."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 037 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 070207_dcs08.pdf attached with page numbers added).

637. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

638. *See id*.

639. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 06 of *1st Consolidated Exhibits* (Dkt. #587-1) (LAESP messages containing real-time cell site sector location information).

systems involves monitoring information, recording it onto digital media, and playback/transcription into a readable document."[640] "Digital Collection Systems are used primarily by FBI field offices and Resident Agencies in support of active foreign intelligence and criminal cases. Support is also provided to other federal, state, local and tribal agencies, as required."[641]

2. DCSNET.

The Digital Collection Systems Network (DCSNET)[642] is the communications medium used by the FBI Digital Collection Systems.[643] DCSNET is a peerless and private encrypted

640. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/082707_dcs05.pdf [EFF PDF Set 5 of 6] (last accessed: Oct. 25, 2010), p. 44 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

641. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

642. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 56 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-5) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

643. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

IP network[644][645] layered over the FBI Trilogy network backbone—an enterprise wide area digital communications network deployed to link all FBI field offices and resident agencies.[646] [647] DCSNET supports the transport and delivery of CALEA based call-identifying information and call content from Telecommunications Service Providers to Digital Collection Systems located at Central Monitoring Plants within FBI offices.[648][649][650] The FBI is in a

644. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080114_dcs04.pdf [EFF PDF Set 4 of 4] (last accessed: Oct. 25, 2010), p. 105 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

645. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071022_dcs03.pdf [EFF PDF Set 3 of 6] (last accessed: Oct. 25, 2010), p. 32-33 of 90; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 042 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).

646. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

647. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 3 of 6], p. 32-33 of 90; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 042 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).

648. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

649. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 56 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

650. A Central Monitoring Plant is a physical area set aside within a building to house Digital

continual relationship with all major Telecommunications Service Providers[651][652] to allow them limited access to DCSNET for the purpose of providing the FBI with call-identifying information and call content associated with the communications of intercept targets.[653][654] Telecommunications Service Providers deliver this information via Call Data Channels (CDCs) and Call Content Channels (CCCs) logically linked[655] to FBI DCSNET gateways[656] from

---

Collection System servers (*e.g.*, the DCS-3000), networking equipment, client PCs, *etc*. *See* FBI Jul. 2, 2007, Response to EFF FOIA Request [EFF PDF Set 8 of 8], p. 90; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 037 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 070207_dcs08.pdf attached with page numbers added).

651. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071022_dcs02.pdf [EFF PDF Set 2 of 6] (last accessed: Oct. 25, 2010), p. 60 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

652. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 38 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

653. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

654. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-62 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

655. *See* Telecommunications Industry Association, TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance* (Arlington, VA: May 31, 2000), § 4.2.3, p. 18-19.

656. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

Intercept Access Points (IAPs) located within telecommunications network infrastructure.[657] Once CDC and CCC information is received at a DCSNET gateway, equipment maintained by FBI staff at the Engineering Research Facility (ERF) Operational Technology Division (OTD) Telecommunications Intercept and Collection Technology Unit (TICTU) Switch-Based Intercept Team (SBIT) distributes the data in real-time to network switches located at Central Monitoring Plants at the appropriate FBI field offices where the data is collected per court orders and/or warrants.[658][659][660]

---

page numbers added).

657. An Intercept Access Point is "a point within a telecommunication system where some of the communications or call-identifying information of an intercept subject's equipment, facilities and services are accessed." TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*, § 3, p. 9. An Intercept Access Point typically consists of a telecommunications network switch. *See id.*, "Annex A," § A.1, p. 82. The switch is connected to a Packet Assembler-Disassembler (PAD) which is in turn connected to a modem with a direct link to a DCSNET gateway. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 58-59 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

658. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 3 of 6], p. 33 of 90 ("The DCSNET is monitored and maintained by staff from the Operational Technology Division's (OTD) Telecommunications Intercept and Collection Technology Unit (TICTU)."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 042 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).

659. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 51 of 74 ("The TICTU's Switch-Based Intercept Team is responsible for distributing this data to the appropriate field offices where it is collected per court orders.... [T]his data is delivered real-time..."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

660. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 38 of 125 ("The TICTU SBIT operations currently network all FBI field offices with realtime

3. The technical specifications outlined in the Telecommunications Industry Association, TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*.

Certain hardware and software elements of the FBI's Digital Collection Program follow the technical specifications outlined in the Telecommunications Industry Association technical standard: TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*.[661] J-STD-025A, which "defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance."[662] According to J-STD-025A, in order to facilitate the collection and delivery of communications content and Pen/Trap data, the FBI and TSPs must implement an Access Function, a Delivery Function, and a Collection Function.[663] The Access Function "consist[s] of one or more Intercept Access Points (IAPs)..."[664] and includes the ability to access intercept subjects' call-identifying information and call content unobtrusively, and make the information available to the Delivery Function.[665] "The Delivery Function is responsible

---

delivery of pen register/trap trace information for all major wireless carriers."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

661. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 123 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

662. *See* TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*, § 1.1, p. 1.

663. *See id.*, § 5.3, p. 34 (Network Reference Model).

664. *Id.*, § 4.2.2, p. 16.

665. *See id.*, § 5.3.1.1, p. 35.

for delivering intercepted communications [(over DCSNET)] to one or more Collection Functions. The Delivery Function delivers information over two distinct types of channels: Call Content Channels (CCCs) and Call Data Channels (CDCs)."[666] "The Collection Function is responsible for collecting and analyzing intercepted communications and call-identifying information [(*i.e.*, Pen/Trap data)][]"[667] sent to it by the Delivery Function. The Collection Function is solely the responsibility of the law enforcement agency.[668] For example, the FBI's primary Collection Function is at its Engineering Research Facility where the collected communications content and Pen/Trap data is forwarded to destination Central Monitoring Plants at the various FBI offices.[669]

Under J-STD-025A, delivery of Pen/Trap data from a wireless carrier Delivery Function is made over a DCSNET Call Data Channel using the Lawfully Authorized Electronic Surveillance Protocol (LAESP)—an Open System Interconnection (OSI) Layer 7 (Application Layer) Protocol.[670] LAESP messages are binary encoded and compatible with the X.208

666. *Id.*, § 4.2.2, p. 17 ("The CCCs are generally used to transport call content, such as voice or data communications. The CDCs are generally used to transport messages which report call-identifying information, such as the calling party identities and called party identities."). However, in the case of packet-mode content information, CDCs are used by the Delivery Function to delivery communications content to the Collection Function. *See id.*, § 5.3.1.2, p. 35.

667. *Id*.

668. *See id*.

669. *See Technical Explanations*, Section III(H)(2), *supra* (explaining DCSNET).

670. *See* TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*, § 6.2.1, p. 61.

Abstract Syntax Notation One (ASN.1) and the X.209 Basic Encoding Rules (BER).[671][672] LAESP messages received by an FBI Central Monitoring Plant are considered the raw and unaltered Pen/Trap data as collected and encoded by an Intercept Access Point belonging to a Telecommunications Service Provider.[673][674] LAESP messages are delivered over Call Data Channels to Central Monitoring Plants using a variety of OSI Layer 2-4 communications protocols including, but not limited to, Transmission Control/Internet Protocol (TCP/IP), Point-to-Point protocol (PPP), Serial Link Internet Protocol (SLIP), Link Access Protocol—Balanced (LAPB), and Link Access Protocol—D-Channel (LAPD).[675] Regardless of the protocol stack, Pen/Trap data sent to the FBI via LAESP messages must be sent in real-time, *i.e.*, within eight seconds of the Intercept Access Point receiving Pen/Trap data from the telecommunications

671. *See id.*, § 6.3.2, p. 62.

672. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 06 of *1st Consolidated Exhibits* (Dkt. #587-1) (example of decoded LAESP messages).

673. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 112 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

674. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071119_dcs01.pdf [EFF PDF Set 1 of 4] (last accessed: Oct. 25, 2010), p. 100 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

675. *See* TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*, "Annex A," § A.5, p. 91-92 (Figure 23, "Possible CDC Protocol Stacks").

network.[676][677] As indicated by a data retention chart created by the Department of Justice, LAESP message data is not listed as being recorded/stored by Telecommunications Service Providers.[678]

4. Digital Collection System 3000 (DCS-3000) server.

The Digital Collection System 3000 (DCS-3000), deployed to Central Monitoring Plants in all FBI field offices and resident agencies,[679] is the FBI's primary Pen/Trap and

676. *See* TIA/EIA/J-STD-025A, *Lawfully Authorized Electronic Surveillance*, § 4.7, p. 31 ("A call-identifying message must be sent from the TSP's IAP to the LEA Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event time-stamped to an accuracy of at least 200 milliseconds.").

677. Depending on the type of circuit used to connect the functions, there is a possibility of the Delivery Function receiving call-identifying information before the Access Function utilizes that information for the purpose of providing wireless service. For example, a looped circuit would result in the prospective Pen/Trap data being switched out of the Access Function as a circuit, looped into the Delivery Function, and then back into the Access Function. *See id.*, Annex A, p. 89 (showing diagram of CALEA network Looped Access); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 056 of *2nd Consolidated Exhibits* (Dkt. #821-3) (diagram attached). In such a case, law enforcement may receive Pen/Trap data before the wireless carrier even utilizes the data to provide service to the intercept subject.

678. *See* Department of Justice, *Retention Periods of Major Cellular Service Providers* (Aug. 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf (last accessed: Dec. 7, 2011) (Neither LAESP messages, call-identifying information, nor Pen/Trap data are listed amongst the data recorded and retained by Verizon Wireless, T-Mobile, AT&T, Sprint, Nextel, and Virgin Mobile.); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 054 of *2nd Consolidated Exhibits* (Dkt. #821-3) (data retention period chart attached).

679. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 3 of 6], p. 32 of 90; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 042 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).

communications content collection system.[680][681] For Pen/Trap data, the DCS-3000 is responsible for processing LAESP messages[682] (containing call-identifying information) sent by Telecommunications Service Provider IAPs as they arrive at FBI Central Monitoring Plants over DCSNET. All major Telecommunications Service Providers have network switches configured to be IAPs capable of generating and sending LAESP messages that are ultimately routed to DCS-3000 servers by SBIT.[683][684] The DCS-3000 is a Microsoft Windows based[685]

680. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/20080114_dcs03.pdf [EFF PDF Set 3 of 4] (last accessed: Oct. 25, 2010), p. 41 of 204 ("The DCS-3000 software suite is the Bureau's primary CALEA pen register collection application..."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 047 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs03.pdf attached with page numbers added).

681. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 22 of 74 ("The DCS-3000 provides access and collection of both call detail information (*i.e.*, pen register and trap/trace) and call content for a variety of telecommunications switches."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

682. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 17 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

683. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 17 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

684. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 38 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

685. *See* FBI Feb. 11, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080211_dcs02.pdf [EFF PDF

[686] server platform comprised of commercial-off-the-shelf hardware[687] and loaded with a custom application suite developed by Booz Allen & Hamilton (BAH)[688][689] under the direction of TICTU.[690] The DCS-3000 server software suite consists of the following applications: (1) Server application (used to collect CDC information pursuant to CALEA);[691]

Set 2 of 3] (last accessed: Oct. 25, 2010), p. 88 of 96 (indicating that "TICTU needs PCAnywhere licenses" (a Microsoft Windows program) to support installations of DCS-3000 systems); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 050 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080211_dcs02.pdf attached with page numbers added).

686. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071022_dcs04.pdf [EFF PDF Set 4 of 6] (last accessed: Oct. 25, 2010), p. 99-100 of 100 (discussing Windows 2000 software for DCS-3000); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

687. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 33 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

688. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 2-3 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

689. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 3 of 4], p. 41 of 204; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 047 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs03.pdf attached with page numbers added).

690. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 21-22 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

(2) Viking application (used to decode audio communications);[692] (4) Enhanced Codec Decoder application (used to decode audio communications);[693] (5) Multivanguard application (used to *(a)* route FISA CDC and CCC information to the DCS-5000 (FISA platform),[694][695][696] *(b)* route Title III (wiretap) CCC information to the DCS-6000 (criminal platform),[697][698] and *(c)* route CALEA CDC information to the DCS-3000 Multiserver application); (6) Multiserver application (used to send collected CALEA CDC information to DCS-3000 client computer workstations located in the same Central Monitoring Plant as the DCS-3000 server);

691. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-62 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

692. *See id*.

693. *See id*.

694. *See id*.

695. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 105 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

696. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 115 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

697. *See id*.

698. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-62 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

[699][700] (7) Tracker application (used to geographically display cell site position based off of CALEA CDC information associated with the communications of an intercept subject);[701] and (8) Backtrack application (used to geographically display cell site position based off of historical cell site location information associated with the communications of an intercept subject).[702] In order to access data collected by a DCS-3000 server, agents use a client software suite consisting of various component applications[703] residing on one or more Microsoft Windows based client computer workstations[704] within the Central Monitoring Plant.[705]

699. *See id*.

700.*See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 17 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

701. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 60-62 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

702. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 85-87 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

703. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 17 of 74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

704. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 149 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

705. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 2 of 6], p. 63 of

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

---

5. DCS-3000 CDNRS Files.

Once the raw and unaltered LAESP messages are received at an FBI Central Monitoring Plant, they are processed and altered by the DCS-3000 into "human readable"[706] text formatted archive files[707] using the "CDNRS" file format.[708][709] While processing the raw and unaltered LAESP messages, the DCS-3000 attempts to extract and format relevant Pen/Trap data before saving it into archive files having .cdnrs file extensions.[710] This post-processed (altered) Pen/Trap data is processed by the DCS-3000 a second time if agent

---

74; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 041 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs02.pdf attached with page numbers added).

706. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 112 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

707. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

708. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 105 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

709. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 46 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

710. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 46 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

instructs the DCS-3000 to save the data into the CDNRS upload file format.[711][712] In response to an agent requesting such a save, the DCS-3000 reformats the Pen/Trap data contained in the .cdnrs files and saves the reformatted data in "summary" and "log" files[713] having .sum and .log file extensions.[714] The DCS-3000 then automatically places the .sum and .log files into folders named "sum" and "log" respectively and places those folders into a second folder named "Cdnrs" nested in a parent folder taking the name of the target phone number[715] (*e.g.*, H:\5551234567\Cdnrs\Log\000000.000.log). The CDNRS .sum and .log files are typically

711. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 5], p. 105 of 150; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 046 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs05.pdf attached with page numbers added).

712. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 75 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

713. *See* FBI Feb. 11, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080211_dcs03.pdf [EFF PDF Set 3 of 3] (last accessed: Oct. 25, 2010), p. 84 of 163; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 051 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080211_dcs03.pdf attached with page numbers added).

714. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 10 of *1st Consolidated Exhibits* (Dkt. #587-1) (example of .sum CDNRS file); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 09 of *1st Consolidated Exhibits* (Dkt. #587-1) (example of .log CDNRS file).

715. *See* FBI Feb. 11, 2008, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20080211_dcs01.pdf [EFF PDF Set 1 of 3] (last accessed: Oct. 25, 2010), p. 20 of 154; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 049 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080211_dcs01.pdf attached with page numbers added).

used to upload the post-processed Pen/Trap data to the Telephone Applications (TA) database[716] at FBI Headquarters.[717]

6. Telephone Applications System.

The Telephone Applications System, maintained by the FBI's Information Technology Operations Division (ITOD),[718] consists of a database of Pen/Trap data and various software applications remotely used by FBI field offices to search and analyze the data contained in the database.[719][720] Most FBI field offices use the DCS-3000 as a front-end collection system for Pen/Trap data.[721] Once the Pen/Trap data is collected, it is converted into the CDNRS upload

716. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 75 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

717. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

718. *See* FBI Feb. 11, 2008, Response to EFF FOIA Request [EFF PDF Set 1 of 3], p. 15 of 154; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 049 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080211_dcs01.pdf attached with page numbers added).

719. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

720. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 111 and 121 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

721. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 121 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd*

file format[722] and then uploaded to the Telephone Applications database located at FBI Headquarters.[723] The task of uploading the CDNRS files to the Telephone Applications database may be done either manually by an agent or automatically by the DCS-3000.[724][725] The Telephone Applications database maintains a record of all Pen/Trap data collected by the FBI since the time the database was created. The Telephone Applications software allow investigators to conduct cross reference and datamining investigations using the database in order to generate leads and display Pen/Trap data in a user friendly form. Agents may use either Trilogy desktop computers or DCS-3000 client computers to access the Telephone Applications database via search and analysis application software.

7. FBI Cell Site Database.

The FBI TICTU/SBIT maintains a large central database containing cell site position

Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

722. *See Technical Explanations*, Section III(H)(5), *supra*.

723. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

724. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 112 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

725. *See* FBI Feb. 11, 2008, Response to EFF FOIA Request [EFF PDF Set 1 of 3], p. 15-20 of 154; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 049 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080211_dcs01.pdf attached with page numbers added).

information for all major wireless carriers.[726][727] The cell site database may be queried by agents to provide the geographic location of a particular target's location based off of either real time Pen/Trap data[728] contained in LAESP messages or historical data[729] obtained directly from wireless carrier personnel. The cell site database contains up to date records of the longitude and latitude coordinates for each wireless carrier cell site and the general cell site sector positioning convention used by each respective wireless carrier, *i.e.*, beamrange and a standard default beamwidth for each sector.[730] For some wireless carriers, the cell site database also contains up to date records on the precise antenna azimuth and beamwidth of

726. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 43 and 93 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

727. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 54 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

728. *See id*.

729. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 42 of 67; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

730. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 93 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

each cell site sector covering the wireless network.[731][732] There are numerous ways that agents may access the cell site database for the purpose of locating wireless devices. Among other means of access, the DCS-3000 has a "software hook" that can be used to automatically send cell site position records from the cell site database to various locally installed mapping programs[733] such as Wintrack[734] by Integrated Systems Research (ISR) and Microsoft Streets and Trips.[735][736] The "software hook" also allows for sending cell site position records from

731. *See id.*, p. 92-96 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

732. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 55 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

733. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 93 of 143 ("There's a hook in the DCS 3000 Client software that can feed [REDACTED] or any other GPS mapping system with cell-site position information in real-time."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

734. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 66-67 of 67; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

735. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 93 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

736. *See* FBI Dec. 17, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/20071217_dcs03.pdf [EFF PDF Set 3 of 5] (last accessed: Oct. 25, 2010), p. 103 of 123; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 045 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071217_dcs03.pdf attached with page numbers added).

the cell site database to other DCS server platforms such as the DCS-1020 used in the FBI "WITT Van" integration project.[737][738]

8. FBI Wireless Intercept and Tracking Team (WITT).

Once cell site location information (either historical or real time)[739] is used to locate a target wireless device to an area covered by a single cell site sector, local FBI Wireless Intercept and Tracking Team (WITT) agents[740] will attempt to pinpoint the location of the

737. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 95 of 143 ("We developed this feature to integrate with our [REDACTED] van-based systems. The idea is to have the DCS 3000 feed lat/long information via cellular modem to a [REDACTED] van."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

738. *See* FBI Sept. 24, 2007, Response to EFF FOIA Request Nos. 1056287-000 & 1056307-1, *available at* http://www.eff.org/files/filenode/061708CKK/092407_dcs01.pdf [EFF PDF Set 1 of 3] (last accessed: Oct. 25, 2010), p. 52-58 of 113 (sections DCS-1020 Software Installation and Users Manual); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 040 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 092407_dcs01.pdf attached with page numbers added).

739. *See* FBI Jan. 14, 2008, Response to EFF FOIA Request [EFF PDF Set 4 of 4], p. 118 of 129; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 048 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20080114_dcs04.pdf attached with page numbers added).

740. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 45-47 of 67; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

device[741][742] by deploying a "WITT Van"[743][744] equipped with a transportable wireless device locator,[745] *i.e.*, the Harris StingRay.[746] The WITT agents will attempt to pinpoint the location of the target wireless device by using the StingRay and related surveillance equipment while driving the WITT Van around the area covered by the previously identified serving cell site sector.[747][748] If agents are collecting call-identifying information on the intercept subject, the

741. *See id.*, p. 41 of 67; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

742. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 54 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

743. *See id.*, p. 36 of 125 ("...DCS-1020 gateway server for the real-time delivery of cell site location information to Wireless Tracking Team (WITT) vans."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

744. *See* FBI Sept. 24, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 3], p. 52-58 of 113 (sections DCS-1020 Software Installation and Users Manual); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 040 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 092407_dcs01.pdf attached with page numbers added).

745. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 41 of 67; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

746. *See Technical Explanations*, Section III(G)(1), *supra* (explaining the StingRay).

747. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 16 and 26 of 67; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

748. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 100 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd*

local Central Monitoring Plant will send the target's cell site sector location/position information to the WITT van in real-time.[749] The local Central Monitoring Plant completes this task through the following chain of events: (1) the DCS-3000 server receives cell site location information for a target[750] via LAESP messages[751] sent from a wireless carrier Intercept Access Point,[752] (2) the DCS-3000 server processes and alters the LAESP messages into the CDNRS file format,[753] (3) the DCS-3000 server queries the cell site database at the FBI ERF over DCSNET for longitude, latitude, azimuth, beamwidth, and beamrange[754][755] of the serving cell site/sector listed in the CDNRS files, (4) once receiving the requested cell site position information, the DCS-3000 server sends the data to a DCS-1020 gateway server[756]

Consolidated Exhibits (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

749. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 36 of 125 ("...DCS-1020 gateway server for the real-time delivery of cell site location information to Wireless Tracking Team (WITT) vans."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

750. *See Technical Explanations*, Section III(H)(4), *supra* (explaining the DCS-3000 server).

751. *See id.*, Section III(H)(3), *supra* (explaining LAESP messages).

752. *See id.*, Section III(H)(2), *supra* (explaining IAPs).

753. *See id.*, Section III(H)(5), *supra* (explaining CDNRS files).

754. *See id.*, Section III(H)(7), *supra* (explaining FBI cell site database).

755. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 93 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

756. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 36 of 125; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page

located at the same Central Monitoring Plant as the DCS-3000, and (5) the DCS-1020 server sends the cell site/sector location/position information over the Internet[757][758] via a Virtual Private Network (VPN),[759] to a wireless cellular modem (*i.e.*, an FBI aircard)[760][761] paired with a laptop computer[762][763] located inside the WITT Van. Once the WITT van receives the real-time cell site location information, WITT agents drive the van around the target area while

numbers added).

757. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 3 of 6], p. 7 of 90; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 042 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 20071022_dcs03.pdf attached with page numbers added).

758. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 61 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

759. *See id.*, p. 55-56 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

760. *See* FBI Nov. 19, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 4], p. 93 of 143; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 044 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071119_dcs01.pdf attached with page numbers added).

761. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 61 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

762. *See* FBI Oct. 22, 2007, Response to EFF FOIA Request [EFF PDF Set 4 of 6], p. 56 of 100; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 043 of *2nd Consolidated Exhibits* (Dkt. #821-3) (relevant pages of 20071022_dcs04.pdf attached with page numbers added).

763. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 5 of 6], p. 54 of 125 ("The DCS-3000 software has been enhanced to push cell site GPS coordinates for specific

using the StingRay to obtain a general, but more precise, location estimate. Once the StingRay obtains the general location, WITT agents will deploy handheld equipment (*i.e.*, the Harris KingFish) to pinpoint the exact location of the target wireless device—even as precise as within a hotel, office building, or similar structure.[764]

IV. How The Aircard Was Intruded Upon

While the FBI's ultimate goal in United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz. was to determine the precise location of the UTStarcom PC5740 1xEV-DO aircard, a number of independent intrusions occurred during the process. The proceeding subsections explain the various ways the FBI intruded upon the aircard, the host laptop computer paired with the aircard, and the home residence of the owner/user of those devices, *i.e.*, apartment No. 1122 at the Domicilio apartment complex.[765] In support of the factual claims outlined in the subsections immediately below, I cite to the *Technical Explanations* above, case discovery and concessions on the record in United States v. Rigmaiden, and public sources of information. In this section, whenever I refer to the aircard's "user," I am referring to myself.

---

targets to a remote tracking laptop of mobile FBI agents."); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 039 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs05.pdf attached with page numbers added).

764. *See* FBI Aug. 27, 2007, Response to EFF FOIA Request [EFF PDF Set 1 of 6], p. 41 of 67; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 038 of *2nd Consolidated Exhibits* (Dkt. #821-2) (relevant pages of 082707_dcs01.pdf attached with page numbers added).

765. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050* (Dkt. #824-2).

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

A. Prerequisite background information.

1. General background information on the aircard, host laptop computer, aircard account, and aircard service.

1. The aircard[766] relevant in United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz. is a "UTStarcom PC5740 Broadband Connection Card For Verizon Wireless"[767] The aircard was used to access a monthly billed Verizon Wireless 1xEV-DO "BroadbandAccess Connect Service" account.[768] The aircard account allowed for accessing the Internet through the Verizon Wireless cellular data network, which is based on the cdma2000 1xEV-DO Rel. 0 technical standards,[769][770] and also had an SMS text message service[771] based on the

766. The government's filings relating to the D.Ariz. 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV applications and court orders, and the N.D.Cal. 08-90330MISC-RS and 08-90331MISC-RS applications and court orders, interchangeably refer to the aircard as the "Target Device," "target broadband access card," "Target Broadband Access Card/Cellular Telephone," "telephone," and other similar terms.

767. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (government web research on aircard).

768. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz. (Dkt. #565-1, p. 11); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection* (Dkt. #824-3, ¶ 7, p. 3-4).

769. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (government web research on aircard indicating that the aircard is not 1xEV-DO Rev. A capable); Qualcomm Inc., EV-DO Rev. A and B: Wireless Broadband for the Masses (whitepaper), *The History of Mobile Broadband* (Dec. 2007), *available at* http://www.qualcomm.com/documents/files/ev-do-rev-and-b-wireless-broadband-masses-whitepaper.pdf, p. 3-4 (last accessed: Dec. 14, 2011) ("EV-DO Release 0 was first launched in 2002" and was later succeeded by EV-DO Rev. A and B.).

770. *See Technical Explanations*, Section III(B), *supra* (listing the primary relevant 3GPP2 cdma2000, 1xEV-DO Rel. 0 technical standards).

771. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz. (Dkt. #565-1, p. 11).

cdma2000 1xRTT technical standards. The associated aircard account did not have cellular telephone service.[772]

2. The aircard is a cellular device that transmits and receives Internet data and text messages (*i.e.*, electronic communications) through a radio transceiver and antenna contained in the device. Specifically, the aircard is a High Rate Packet Data (HRPD) 1xEV-DO Rel. 0 Access Terminal[773] with hybrid[774] 1xRTT text message service and low rate data service capabilities. The aircard hardware is incapable of ringing or alerting to an incoming call and it does not allow for placing or receiving telephone calls (*i.e.*, wire communications).[775] Unlike cellular telephones that have built into their hardware "a compact speaker, a microphone, a keyboard, [and] a display screen...,"[776] the aircard is a personal computer hardware "add-on card" that can only function when plugged into the PCMCIA slot of a host laptop computer.[777]

3. The host laptop computer used with the aircard was an IBM ThinkPad (S/N #LV-

772. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 13 of *1st Consolidated Exhibits* (Dkt. #587-1) (on June 26, 2008, FBI Agent Murray was advised by Verizon Wireless that the aircard does not have telephone service).

773. *See Technical Explanations*, Section III(B)(2)(a), *supra* (explaining 1xEV-DO Rel. 0 Access Terminals).

774. *See Technical Explanations*, Section III(B)(3)(g)(ii), *supra* (explaining 1xEV-DO Rel. 0 Hybrid Access Terminals (HAT) operations).

775. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (government web research on aircard).

776. CTIA [website], *How Wireless Works*, http://www.ctia.org/consumer_info/index.cfm/AID/10324 (last accessed: Dec. 7, 2011) (explaining how cell phones work).

777. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (government web research on aircard).

C4398) laptop computer (hereafter "host laptop computer" or "home computer") with mouse, docking station, external LCD monitor, external keyboard, and external hard drives.[778][779] In order to function, the aircard drew power from the host laptop computer, stored data on the hard drive of the host laptop computer, and its functions and operations were accessed through software installed on the host laptop computer.[780]

4. Whenever the aircard was plugged into the host laptop computer, the user would immediately initialize a connection with Verizon Wireless and then take measures to ensure that the connection would reconnect upon a disconnect.[781] In order to connect to Verizon Wireless and access the Internet, either the host laptop computer operating system software compatible with the aircard would be used or the VZAccess Manager software bundled with the aircard would be used.[782] While accessing the Internet, radio waves were transmitted to/from the aircard and the cell sites that were part of the Verizon Wireless 1xEV-DO Rel. 0 data network.

778. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Materials Related To Search Warrant No. 08-70460, Authorized By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30, 2008* (return) (Dkt. #464-1).

779. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection* (Dkt. #824-3, ¶ 4, p. 2-3).

780. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 11 of *1st Consolidated Exhibits* (Dkt. #587-1) (government web research on aircard indicating that the aircard is bundled with VZAccess Manager software); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection* (Dkt. #824-3, ¶ 17, p. 6-7).

781. *See id.*, ¶ 17-20, p. 6-7.

782. *See id.*, ¶ 17, p. 6-7.

[783] The radio waves sent between the aircard and the Verizon Wireless 1xEV-DO Rel. 0 data network carried the signals that communicated data between the host laptop computer and the Internet.[784]

2. Basis for concluding that the government used the Harris StingRay, KingFish, and related equipment to locate the aircard and its user.

a. The government admitted that FBI technical agents used the Harris StingRay to locate the aircard.

5. The government refuses to disclose detailed discovery to the defense in United States v. Rigmaiden relating to the portable/transportable wireless device locators used to locate the aircard. Likewise, the Court refuses to order the government to produce the sought after evidence.[785] However, the government has already identified one piece of equipment used to locate the aircard: the StingRay manufactured by Harris.[786][787] In a report of investigation

783. *See Technical Explanations*, Section III(B) *et seq.*, *supra* (explaining aspects of a 1xEV-DO Rel. 0 cellular data network).

784. *See id*.

785. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court Order* (Dkt. #723, p. 13) (Denying the defendant's motion for disclosure (Dkt. #592) and noting that "[d]isclosing the particular equipment used, and how it was used, would disclose how the FBI seeks to track mobile electronic devices such as the aircard. Even if some of the technology were publicly available, the precise technology used by the FBI in this case and the precise manner in which it was used, if disclosed, would educate the public and adversaries of law enforcement on how precisely to defeat FBI surveillance efforts.").

786. *See Technical Explanations*, Section III(G) *et seq.*, *supra* (explaining technical details of the Harris StingRay).

787. Even if the government used portable/transportable wireless device locators that were not the Harris products, the operations of the actual devices used will be similar to the operations of the Harris products. For example, any portable/transportable wireless device locator seeking to locate a 1xEV-DO Rel. 0 wireless device in cell site emulator mode must

disclosed to the defense, USPIS Inspector James L. Wilson stated that FBI technical agents were "using a '**Stingray**' to pinpoint the location of the aircard."[788] Furthermore, in rough notes disclosed to the defense, IRS-CI Agent Denise L. Medrano created a "to-do list" containing the "**S**ting**R**ay" term in CaSe-CoRrEcT fashion.[789][790]

6. After realizing that use of the Harris StingRay was revealed to the defense in United States v. Rigmaiden, the lead prosecutor, AUSA Frederick A. Battista claimed, without presenting any evidence, that the term "StingRay" is a generic term used by law enforcement to

follow all of the procedures outlined in the *Technical Explanations*, Sections II(B) *et seq.*, *supra* (addressing the 1xEV-DO Rel. 0 communications protocol). Additionally, geolocation of radio frequency signals discussed in the *Technical Explanations* is a well defined science.

788. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 26 of *1st Consolidated Exhibits* (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson) (emphasis added).

789. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 109 of *2nd Consolidated Exhibits* (Dkt. #821-6) (July 15, 2008 rough notes by IRS-CI Agent Medrano).

790. Harris spells "StingRay" with a capital "S" and a capital "R" in the same way IRS-CI Agent Medrano used the term on her list. IRS-CI Agent Medrano did not use such capital spelling style for any other listed phrase.

refer to any type of surveillance equipment capable of locating wireless devices.[791][792] AUSA Battista specifically claimed that USPIS Inspector Wilson and IRS-CI Agent Medrano used the term "StingRay" generically and that the primary case agents neither saw nor learned of the equipment used to locate the aircard.[793]

7. Contrary to AUSA Battista's claims, FBI Agent Richard J. Murray (a primary

---

791. The government made this claim via AUSA Battista during the September 22, 2011 court hearing:

> MR. BATTISTA: I've sought to explain to Mr. Rigmaiden, and the example I use, and I talked about this case so many times, is Kleenex and tissue. Kleenex is a brand name but it's a tissue. People regularly refer to tissue as Kleenex. "I need to blow my nose. Will you give me a Kleenex?" Everyone knows what they're talking about.
>
> In the law enforcement world, there's a StingRay and then there's the generic term "StingRay" meaning all types of devices. The five case agents were using the term "StingRay" as the term "Kleenex." They did not operate the equipment. They did not know what the equipment is. They didn't receive any training on the equipment.
>
> United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *September 22, 2011 Status Conference, Partial Transcript of Proceedings* [MR. BATTISTA], p. 36.

792. The word "StingRay" (or "stingray") is not, in fact, a generic term for "cell site emulator" or "cell site simulator." A government document produced via a FOIA request does not list "StingRay" as one of the many generic terms used to refer to portable/transportable wireless device locators. *See* USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, p. 18 of 42 (listing "digital analyzer, cell site locator, triggerfish, ESN reader, or swamp box" as generic terms used to refer to cell site simulators); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 021 of *2nd Consolidated Exhibits* (Dkt. #821-1) (relevant pages of cellfoia_release_074130_20080812.pdf attached with page numbers added).

793. The claim made by AUSA Battista during the September 22, 2011 court hearing is as follows:

> So they were -- in the course of the investigation, the term "StingRay" was

case agent) stated in two "case write ups" that he conducted a test with the IRS involving the geolocation of a similar aircard prior to FBI technical agents locating the actual aircard:

> I worked with the AUSA and the FBI SF to obtain a pen register and tracking court order to locate the aircard with TTA [(*i.e.*, FBI Technically Trained Agent)] assistance. I ran a field test with IRS of a similar aircard and communicated with OTD to ensure that the tracking would not be detected by the subject.
>
> *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 065 of *2nd Consolidated Exhibits* (Dkt. #821-3) (Feb. 28, 2009 "case write up" by FBI Agent Murray).

The above quoted "case write up" is corroborated by a text message sent by FBI Agent Murray to FBI Agent Kevin F. Killigrew on July 16, 2008 at 1:46am.[794] Because the primary case agents were aware of the precise make and model of the equipment used, the references in the discovery to the StingRay refer to the Harris StingRay.

> used as a generic term. I've explained this to the defendant numerous times. None of the five investigators know the make, model, manufacturer of the exact equipment. There were tech agents out there. They're the ones who possessed the equipment, operated the equipment.
>
> So, yes, the word "StingRay" is in the discovery. When they're using the term "StingRay," and I've explained this to the defendant, it's Kleenex. It's tissue. They don't know. It could be a StingRay. It could not be. It could be something else. They didn't know what it was. They didn't see it. They didn't operate it.
>
> *September 22, 2011 Status Conference, Partial Transcript of Proceedings* [MR. BATTISTA], p. 36.

794. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 063 of *2nd Consolidated Exhibits* (Dkt. #821-3) (July 16, 2008, 1:46am, text message sent from FBI Agent Murray to FBI Agent Killigrew: "We verified the ability to pull the card over through testing on an irs verizon card. Atech agent from [REDACTED: TTA First Name], is here helping out and he has top game.").

b. Heuristics and process of elimination confirms that FBI technical agents used the Harris StingRay, KingFish and AmberJack to locate the aircard.

8. FBI Supervisory Agent Bradley S. Morrison confirmed that the "equipment used to locate the defendant's aircard did not capture, collect, decode, view, or otherwise obtain any content transmitted from the aircard, and therefore was unable to pass any of this information from the aircard to Verizon Wireless [(*i.e.*, no communication interception)]."[795][796] The prosecution thereafter stated that the equipment used to locate the aircard was **incapable** of intercepting and forwarding aircard communications content.[797] Through process of elimination, the surveillance equipment used to locate the aircard must be limited to solely having geolocation capabilities. While there are numerous air interface surveillance devices available from various manufacturers, only Altron, NeoSoft, MMI, and Harris manufacture devices specifically designed to not have the ability to intercept communications and conduct man-in-the-middle attacks.[798]

795. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Government's Memorandum Re Motion For Discovery*, "Affidavit Of Supervisory Special Agent Bradley S. Morrison," ¶ 4, p. 2-3 (Dkt. #674-1, p. 2-3).

796. Note: Unless otherwise noted, I do not agree with FBI Agent Morrison's technical conclusions and other claims in his affidavit.

797. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 071 of *2nd Consolidated Exhibits* (Dkt. #821-4) (December 2, 2011 letter from AUSA Battista to the defendant, p. 2: "[T]he FBI equipment used in your case could not be used to conduct a 'man in the middle' attack.").

798. *See Technical Explanations*, Section III(G), *supra* (explaining how technical data on air interface surveillance equipment manufactured by Ability, Meganet, Shoghi Communications Ltd., Verint, and View Systems indicate an ability to conduct man-in-the-middle attacks while technical data on certain models of air interface surveillance equipment manufactured by Altron, NeoSoft, MMI, and Harris indicate no such capabilities).

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

9. Through further process of elimination, the only possible manufacturer of the equipment used to locate the aircard is Harris. It is undisputed that in order to "track the signals from the aircard, the FBI used [][equipment] that functions as a cell site simulator. The equipment mimicked a Verizon Wireless cell tower and sent and received signals directly to and from the aircard."[799] It is also undisputed that the aircard is a cdma2000 based wireless device, *i.e.*, compatible with the 1xEV-DO Rel. 0 and 1xRTT air interface standards.[800] Out of all cell site emulator capable air interface surveillance equipment sold by Altron, NeoSoft, MMI, Harris, Ability, Meganet, Shoghi Communications Ltd., Verint, and View Systems—only the Harris StingRay and KingFish support cdma2000 based air interface standards (*e.g.*, 1xEV-DO Rel. 0 and 1xRTT as used by the aircard).[801] Through process of elimination, the only portable/transportable wireless device locators that are technologically capable of locating the aircard are the Harris StingRay and KingFish.

10. The government also effectively conceded that the FBI used two separate wireless device locators to locate the aircard. The government stated that "[t]he FBI used the [locating] equipment in multiple locations... [but] it never used more than a single piece of

799. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Government's Response To Motion For Discovery* (Dkt. #602, p. 3).

800. S*ee How The Aircard Was Intruded Upon*, Section IV(A)(1), *supra* (explaining how the aircard communicates with the Verizon Wireless 1xEV-DO Rel. 0 and 1xRTT cellular networks).

801. *See Technical Explanations*, Section III(G), *supra* (other than for Harris equipment, all off-the-shelf cell site emulator capable air interface surveillance devices only support surveillance of UMTS and/or GSM based wireless devices).

equipment at any given time."[802] It logically follows that the government's concession means that the FBI used more than one device but not at the same time. Additionally, the government conceded that "[d]uring a portion of the tracking operation, the FBI used handheld equipment from within the Domicilio apartment complex."[803] Although the FBI initially used the StingRay, it is designed to be transportable via a land or air vehicle;[804] therefore, the FBI needed to use a second, handheld wireless device locator while on foot within the Domicilio apartment complex. The Harris KingFish is the only handheld man-portable wireless device locator that operates in cooperation with the Harris StingRay.[805] It logically follows that the FBI would use the KingFish along with the StingRay, as apposed to using a handheld device not designed for cooperative operation with the StingRay.

11. The standard antenna used with the StingRay is the AmberJack phased array beam-forming antenna.[806] The datasheet for the StingRay indicates that it operates with the AmberJack[807] and the datasheet for the AmberJack indicates that it operates with the StingRay.

802. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Government's Response To Motion For Discovery* (Dkt. #602, p. 3).

803. *Id*.

804. *See Technical Explanations*, Section III(G)(1), *supra* (explaining how the StingRay is vehicle-transportable as apposed to man-portable).

805. *See id.*, Section III(G), *supra*.

806. *See id.*, Section III(G)(1)(a)(iii), *supra* (explaining the AmberJack phased array beam-forming antenna used with the StingRay).

807. *See* Miami, FL, USA – Legislative Files, **Harris StingRay Product Datasheet**, p. 1; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 003 of *2nd Consolidated Exhibits* (Dkt. #821-1) (datasheet attached).

[808] Because the AmberJack is the standard antenna used with the StingRay, and because the FBI technical agents used the StingRay to locate the aircard, they also used the AmberJack to locate the aircard.

B. The government's mission to locate the aircard and its user within a private home residence.

1. The government identified the aircard and seized destination IP addresses relating to the aircard user's Internet activity.

12. Based on an unrelated aspect of the investigation,[809] the government identified Verizon Wireless network IP addresses 75.209.101.132, 75.208.105.186, and 75.209.41.104 as being possible end-source IP addresses responsible for submitting three of the allegedly fraudulent e-filed tax returns relating to the investigation in United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz. In June of 2008, the government served Verizon Wireless with D.Ariz. Grand Jury subpoena Nos. 07-03-609 and 07-03-615 requesting identifying information on the customer account and wireless device assigned the three source IP addresses noted above.[810]

13. On June 13, 2008, Verizon Wireless responded to the government's request and

808. *See* Miami, FL, USA – Legislative Files, **Harris AmberJack Product Datasheet**, p. 6-7; *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 011 of *2nd Consolidated Exhibits* (Dkt. #821-1) (AmberJack datasheet attached).

809. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 065 of *2nd Consolidated Exhibits* (Dkt. #821-3) ("[T]hrough separate investigative means, [][FBI Agent Murray] and other agents analyzed ISP IP records and identified the Internet aircard used by the subject...").

810. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Documents Related To District Of Arizona Grand Jury Subpoenas 07-03-609 And 07-03-615 Obtained To Facilitate Locating The Aircard* (Dkt. #565-1, p. 4).

provided identifying information on the aircard and aircard account.[811][812] In the subpoena response, Verizon Wireless also provided the government with approximately 411,257 destination IP addresses pertaining to websites and other Internet resources accessed by the aircard.[813][814][815]

14. By June 25, 2008, the government had matched up a list of IP addresses associated with various e-filed tax returns to some of the aircard destination IP addresses listed in the Verizon Wireless subpoena responses.[816] Based on the match up, the government was convinced that the aircard was responsible for perpetuating the alleged scheme.[817] On July 1,

811. *See id*.

812. Although agents obtained identifying information for the aircard and aircard account, they were unable to determine the location of the aircard and its user.

813. *See id*.

814. On June 18, 2008, the government obtained an additional 111 aircard destination IP addresses accessed by the aircard. *See id*.

815. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Internet activity reflected by the 1,836,140 aircard destination IP addresses seized by the government* (Dkt. #824-4).

816. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 078 of *2nd Consolidated Exhibits* (Dkt. #821-4) (June 25, 2008 email from IRS-CI Agent Daun to FBI Agent Murray *et al.*: "based on the pattern following along for just all of the Ips that I found to match - I really think this is the person filing the returns..."). *See also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 14 of *1st Consolidated Exhibits* (Dkt. #587-1) (July 1, 2008 email from IRS-CI Agent Daun to Nathan A. Watt: "We have correlated returns being filed from specific Proxy Ips, that this guy was also connected to at the same time."); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 15 of *1st Consolidated Exhibits* (Dkt. #587-1) (July 7, 2008 email from IRS-CI Agent Medrano to Constance M. Davis: "We strongly believe we have identified the [][suspect]...").

817. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122*, Application, p. 17-25 (Dkt. #566-1, p.

2008, the government began to prepare and execute plans to use historical cell site location information, real-time cell site location information, and Harris brand portable/transportable wireless device locators to "ping and triangulate on a cellular broadband card we are 99% sure is him."[818]

15. After investigators had relied upon the destination IP addresses to investigate the aircard and its user for a period of 26 days, AUSA Battista learned that it was illegal for the government to use Grand Jury subpoenas to compel disclosure of the destination IP addresses[819] and that subpoenas only allow for disclosure of source IP addresses.[820] On July 8, 2008, AUSA Battista instructed the investigation team to place all aircard destination IP addresses into sealed envelopes[821] and then subsequently applied for a "retroactive order" to

19-27) (explaining government's use of the aircard destination IP addresses to link aircard to e-filed tax returns).

818. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 14 of *1st Consolidated Exhibits* (Dkt. #587-1) (July 1, 2008 email from IRS-CI Agent Daun to Nathan A. Watt); s*ee also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 16 of *1st Consolidated Exhibits* (Dkt. #587-1) (July 7, 2008 email from IRS-CI Agent Daun to IRS-CI Agent Willert: the FBI plans to "triangulate down on the [][suspect's] broadband access card with Verizon in San Jose.").

819. *See* 18 U.S.C. § 2703(c)(2) *et seq.* (allowing the government to obtain "records of session times and durations" and "any temporarily assigned network address" but not destination IP addresses).

820. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 17 of *1st Consolidated Exhibits* (Dkt. #587-1) (on July 7, 2008, USDOJ Office of Enforcement Operations notified AUSA Battista of an "issue" with the aircard destination IP addresses); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard* (Dkt. #576-1).

821. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 18 of *1st Consolidated Exhibits* (Dkt. #587-2) (July 8, 2008 email from AUSA Battista to all primary

unseal the envelopes.[822] On July 9, 2008, the "retroactive order" was granted[823] and the government then continued with its plan to use various geolocation techniques to obtain the precise location of the aircard and its user.[824]

2. The government seized aircard historical cell site location information and conducted historical triangulation / location signature techniques.

16. In July of 2008, the government served Verizon Wireless with the D.Ariz. 08-3298MB-LOA order requesting historical cell site information relating to connections made by the aircard to Verizon Wireless cell sites.[825] On July 12, 2008, Verizon Wireless responded to the D.Ariz. 08-3298MB-LOA order by emailing Robert Byrne, LEO, and FBI Agent Murray historical cell site information pertaining to the aircard and generated during the date range of

case agents: "Please place[] in a sealed envelope all copies of destination IP addresses and... discontinue any use of the information..."").

822. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard* (Dkt. #576-1).

823. *See id*. In addition to effectively unsealing the approximate 411,375 destination IP addresses illegally obtained via subpoena, the government also used the order to obtain an additional 1,424,773 destination IP addresses pertaining to websites and other Internet resources accessed by the aircard. *See id*.

824. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 19 of *1st Consolidated Exhibits* (Dkt. #587-2) (July 11, 2008 email from Albert A. Childress to Brad Taylor *et al.*: the FBI will be able triangulate the suspect's location through use of a portable/transportable wireless device locator).

825. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard* (Dkt. #576-3).

June 10, 2008 through July 11, 2008.[826]

17. Although the order only authorized obtaining historical cell site information to determine the network's *registration* of the aircard, the government obtained historical cell site **location** information showing the network's geographical location of the aircard, *i.e.*, locations of cell sites where the aircard established sessions with the 1xEV-DO Rel. 0 cellular data network.[827] The information provided by Verizon Wireless indicated that the aircard had been historically located within signal range of the following cell sites:

(1) Cell site # 5; Latitude: 37.369733; Longitude: -121.923442; Street address: 2001 Gateway Place, San Jose, CA 95110;

(2) Cell site # 139; Latitude: 37.34955; Longitude: -121.943435; Street address: 900 Lafayette St, Santa Clara, CA 95050;

(3) Cell site # 153; Latitude: 37.418053; Longitude: -121.85978; Street address: 10000 Old Piedmont Rd., San Jose, CA 95132;

(4) Cell site # 268; Latitude: 37.346481; Longitude: -121.923164; Street address: 1070 Elm St, San Jose, CA 95126;

(5) Cell site # 279; Latitude: 37.3416; Longitude: -121.947941; Street Address: 490 Lincoln St., Santa Clara, CA 95050;

The historical cell site location information allowed the government to determine that the

826. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 02 of *1st Consolidated Exhibits* (Dkt. #587-1).

827. *See Technical Explanations*, Section III(B)(3)(c)(ii), *supra* (explaining the 1xEV-DO Rel. 0 session establishment process).

aircard was previously located within signal range of five cell sites covering parts of San Jose and Santa Clara, CA.[828][829]

18. As explained in the *Technical Explanations*, Section III(B)(3)(c)(vi), *supra*,[830] 1xEV-DO Rel. 0 wireless devices such as the aircard do not "register" with cell sites (*i.e.*, Access Networks)—instead, they establish "sessions"[831] and conduct "route updates"[832] with both operations being associated with the IPv6 address identifying the cell site sector. 1xEV-DO Rel. 0 registration occurs separate from cell sites, over the A11 Interface, and does not involve location information as may be relevant to "registration" in the context of GSM and other non IP based mobile networks.[833]

828. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 20 of *1st Consolidated Exhibits* (Dkt. #587-2) (July 14, 2008 email from AUSA Battista to AUSA Yen: the government is looking for the aircard in the area of San Jose International Airport and Santa Clara University).

829. On July 31, 2008, Verizon Wireless responded to the D.Ariz. 08-7273MB-LOA order by providing similar aircard historical cell site location information generated during the date range of June 11, 2008 through July 17, 2008. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 05 of *1st Consolidated Exhibits* (Dkt. #587-1); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Documents Related To District Of Arizona Court Orders 08-3286MB-LOA, 08-3298MB-LOA, and 08-7273MB-ECV Obtained To Facilitate Locating The Aircard* (Dkt. #576-5). Additionally, On August 1, 2008, John Profaca provided a second set of cell site information in response to a direct request made by FBI Agent Murray under the authority of the D.Ariz. 08-3298MB-LOA order. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 03 of *1st Consolidated Exhibits* (Dkt. #587-1).

830. *See also* fn. No. 347, *supra*.

831. *See Technical Explanations*, Section III(B)(3)(c)(iii), *supra*.

832. *See id.*, Section III(B)(3)(d) *et seq.*, *supra*.

833. *See id.*, Section III(B)(3)(c)(vi) and fn. No. 347, *supra*.

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

19. As an initial matter, the historical cell site location information provided by Verizon Wireless allowed the government to determine that the aircard was in a stationary location from June 10, 2008 to July 11, 2008.[834]

20. On the morning of July 14, 2008,[835] FBI Agent Killigrew created a cell tower range chart/map consisting of a street map, plotted Verizon Wireless cell site sectors belonging to cell site Nos. 268, 139, and 279, and a triangulated aircard location signature estimate represented by a shaded area.[836] On the chart/map, the total land area collectively covered by cell site Nos. 268, 139, and 279 is approximately *105,789,264 ft²*.[837] FBI Agent Killigrew used triangulation techniques and location signature techniques to eliminate **93.9%** of that

834. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 35 of *1st Consolidated Exhibits* (Dkt. #587-3) (IRS-CI Agent Medrano rough notes stating that the aircard was accessing the "same tower in San Jose 90% [of the time]" and it "appears not moving[.]"); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 20 of *1st Consolidated Exhibits* (Dkt. #587-2) (July 14, 2008 email from AUSA Battista to AUSA Yen: "the initial Cell Site data" has the government "looking at the area around San Jose International Airport and Santa Clara University.").

835. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 068 of *2nd Consolidated Exhibits* (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: "[P]lease be advised that it appears that the cell tower range chart was created the morning of July 14, 2008, and then shared with the investigation team after 1:00 p.m. that same date.").

836. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 21 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map showing a *6,412,224 ft²* triangulated location signature estimate (marked with black pen lines) covering the location of apartment No. 1122); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map with government's *6,412,224 ft²* triangulated location signature estimate marked in red and apartment No. 1122 marked with a yellow star).

837. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 23 of *1st Consolidated Exhibits* (Dkt. #587-2) (mathematical equation information for calculating the square footage of overlapping signal coverage areas of multiple cell sites and cell site sectors).

105,789,264 ft² area resulting in the location estimate being reduced to *6,412,224 ft²* represented by the shaded area. The shaded area on the cell tower range chart covers the location of apartment No. 1122 at the Domicilio apartment complex.[838]

21. FBI Agent Killigrew's triangulation techniques and location signature techniques consisted of the following steps: (1) obtaining aircard historical cell site location information for June 10, 2008 through July 11, 2008,[839] (2) using the latitude and longitude coordinates of three of the five cell sites (cell site Nos. 268, 139, and 279) contained in the historical cell site location information to plot the cell site locations on a digital/computerized street map,[840] (3) using prior knowledge of Verizon Wireless cell site signal ranges (*i.e.*, antenna radiation patterns) to draw signal range circles around each of the three cell site locations plotted on the digital/computerized street map,[841] (4) using prior knowledge of typical Verizon Wireless cell

838. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map with government's *6,412,224 ft²* triangulated location signature estimate marked in red and apartment No. 1122 marked with a yellow star).

839. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 25 of *1st Consolidated Exhibits* (Dkt. #587-2) (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: FBI Agent Killigrew indicating that he "took the historical cell site data that the cellular provider provided to [][FBI Agent Murray]" in order to create the cell tower range chart/map.).

840. *See id.* (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: "The historical data provided several cell towers with their latitude and longitude. I plotted these on the map by lat/lon.").

841. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 068 of *2nd Consolidated Exhibits* (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: AUSA Battista indicating that FBI Agent Killigrew informed FBI Agent Murray on March 31, 2011 that, "For this particular case I used my knowledge of Verizon wireless cell tower layouts from working previous cases and previous training.").

site sector orientations (*i.e.*, sector azimuths at 0º, 120º, and 240º with sector radiation patterns covering 300º-60º, 60º-180º, and 180º-300º)[842] to draw lines separating each of the noted signal range circles into three sectors each,[843] (5) using the historical cell site location information to calculate which two cell sites were being accessed by the aircard most often (*i.e.*, cell site Nos. 268 and 139)[844] and then weighting the respective signal range circle of the remaining cell site (*i.e.*, cell site No. 279) with a confidence value of -1 (*i.e.*, the aircard is absolutely NOT in the estimated area),[845] (6) using the digital/computerized street map to calculate an overlapping signal range area for the two cell sites used by the aircard most often (*i.e.*, cell site Nos. 268 and 139),[846] (7) using the digital/computerized street map to calculate

842. *See id.* (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: AUSA Battista indicating that FBI Agent Killigrew informed FBI Agent Murray on March 31, 2011 that, "Generally speaking, in urban areas Verizon Azimuths are 0, 120, and 240 degrees. The sectors then encompass 300-60, 60-180, and 180-300.").

843. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 25 of *1st Consolidated Exhibits* (Dkt. #587-2) (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: "After the towers were plotted, using my past experience and training in dealing with cellular networks, I drew circles around the towers that provided for overlapping areas of cellular coverage.").

844. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 02 of *1st Consolidated Exhibits* (Dkt. #587-1) (historical cell site location information showing that the aircard was accessing cell site Nos. 268 and 139 most often); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 25 of *1st Consolidated Exhibits* (Dkt. #587-2) (January 7, 2011 email from FBI Agent Killigrew to FBI Agent Murray: "The tower data provided by the wireless company showed that three towers were hit most often, with one of the three hit significantly more often than the other two.").

845. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (labeled cell tower range chart/map showing nearly no shade lines over sector signal coverage area belonging to cell site No. 279).

846. *See id.* (labeled cell tower range chart/map showing cell site Nos. 268 and 139 having signal coverage areas overlapping).

the three overlapping sector regions within the overlapping signal range area described in No. 6 above,[847] (8) weighting two of the noted three overlapping sector regions covering non residential areas (*i.e.*, the airport as shown on the noted cell tower range chart/map) with a confidence value of -1 (*i.e.*, absolutely NOT containing the location of the aircard),[848] and (9) weighting the remaining overlapping sector region (*i.e.*, the shaded area on the cell tower range chart/map) with a confidence value of 1 (*i.e.*, the aircard is absolutely within the corresponding estimated area).[849] The shaded area on the cell tower range chart/map represents a government triangulated aircard location signature based off of the above explained geolocation techniques.

22. FBI Agent Killigrew's geolocation techniques fit the definition of cell site triangulation as explained by Judge Kaplan.[850] For the triangulation calculation represented

847. *See id.* (labeled cell tower range chart/map showing overlapping sectors from cell site Nos. 268 and 139 creating three separate overlapping sector regions).

848. *See id.* (labeled cell tower range chart/map showing no shade lines over sectors from cell site Nos. 268 and 139 that cover the airport); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 070 of *2nd Consolidated Exhibits* (Dkt. #821-4) (June 18, 2010 letter from AUSA Battista to the defendant, p. 4-5: "The three circles represent estimates of the range of the noted cell towers taking into consideration multiple factors, primarily the distance between the towers and **the terrain**." (emphasis added)).

849. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 21 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map showing a *6,412,224 ft²* triangulated location signature estimate (marked with black pen lines) covering the location of apartment No. 1122); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map with government's *6,412,224 ft²* triangulated location signature estimate marked in red and apartment No. 1122 marked with a yellow star).

850. *See Technical Explanations*, Section III(D)(3), *supra* ("In the context of cell site information, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is discerned from the information

by the shaded area on the cell tower range chart/map, the two known points are cell sites No. 139 and 268, the third unknown point is the aircard, and the south-east sector of cell site No. 139 and the south-west sector of cell site No. 268 are the angles used to complete the equation. [851]

23. FBI Agent Killigrew's geolocation techniques also fit the definition of a location signature calculation using a statistical database containing historical cell site location information and heuristics similar to what is explained by inventors of location signature technology.[852] The statistical database used by FBI Agent Killigrew was the aircard's historical cell site location information (seized from Verizon Wireless) covering the date range of June 10, 2008 through July 11, 2008. FBI Agent Killigrew's location signature techniques allowed for determining (1) the precise cell site sectors accessed by the aircard for use in the triangulation calculation,[853] (2) the specific regions within those sectors accessed by the aircard (*e.g.*, elimination of the terrain covering the airport),[854] and (3) confirmation that the

about which face of each tower is facing the phone." (quoting district Judge Kaplan)).

851. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (labeled cell tower range chart/map).

852. *See Technical Explanations*, Section III(D)(3), *supra* (explaining location signature techniques that take into consideration the terrain, historical cell site location information, weighting of data for confidence values, *etc.* to separate cell site sectors into regions for location signatures).

853. Verizon Wireless only provided the cell sites accessed by the aircard and not the cell site sectors. Through location signature techniques, FBI Agent Killigrew was able to determine the precise sectors accessed by the aircard so that a triangulation calculation could be conducted.

854. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 22 of *1st Consolidated Exhibits* (Dkt. #587-2) (labeled cell tower range chart/map showing no shade lines over sectors from cell site Nos. 268 and 139 that cover the airport).

aircard remained in a stationary position over time.

3. The primary case agents flew from Arizona to California to triangulate the precise location of the aircard and its user.

24. On July 15, 2008, one day after receiving FBI Agent Killigrew's triangulated aircard location signature estimate,[855] FBI Agent Murray, IRS-CI Agent Medrano, IRS-CI Agent Fleischmann, IRS-CI Agent Tracy L. Daun, and USPIS Inspector Wilson (previously and hereafter collectively the "primary case agents") "flew to Santa Clara/San Jose to start triangulating the suspect's position."[856] Upon their arrival, the primary case agents met with FBI Agent Ng at the Campbell FBI field office and later "met with several FBI agents with their Technical Service Division to help [][them] track the suspect's aircard."[857]

25. While in California, the primary case agents employed the help of three FBI technical agents[858] from San Francisco to conduct the real-time portion of the aircard locating mission.[859] The FBI technical agents were members of a Wireless Intercept and Tracking

855. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 068 of *2nd Consolidated Exhibits* (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: "[P]lease be advised that it appears that the cell tower range chart was created the morning of July 14, 2008, and then shared with the investigation team after 1:00 p.m. that same date.").

856. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 26 of *1st Consolidated Exhibits* (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).

857. *Id*.

858. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 073 of *2nd Consolidated Exhibits* (Dkt. #821-4) (December 16, 2011 letter from AUSA Battista to the defendant, p. 1: AUSA Battista making reference to "two of the three tech agents...").

859. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 065 of *2nd Consolidated Exhibits* (Dkt. #821-3) (Feb. 28, 2009 "case write up" by FBI Agent Murray indicating that he "worked with the AUSA and the **FBI SF** to obtain a pen register and tracking

Team (WITT),[860] which uses aspects of the FBI Digital Collection Program to locate wireless devices.[861] The prosecution has not provided the defense with the identities of three FBI technical agents.[862]

4. The FBI technical agents began the real-time portion of the aircard locating mission by conducting base station surveys of all cell sites located in the area covered by the cell tower range chart/ map.

26. Prior to the real-time portion of the aircard locating mission, the FBI technical agents loaded CDMA communications protocol firmware onto their StingRay and KingFish (if not loaded previously).[863][864] The firmware is provided by Harris[865] and was loaded onto the

court order to locate the aircard with TTA assistance." (emphasis added)); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 066 of *2nd Consolidated Exhibits* (Dkt. #821-3) (FBI technical agent memorandum stating that "Phoenix Division requested assistance from San Francisco in locating a target wireless aircard.").

860. *See id.* (FBI technical agent memorandum explaining use of portable/transportable wireless device locators and indicating: "Personnel Performing Mission: TTA-WITT").

861. *See Technical Explanations*, Section III(H)(8), *supra* (explaining FBI WITT).

862. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court Order* (Dkt. #723, p. 12) (The Court denied the defendant's motion for disclosure (Dkt. #592) and concluded that "[d]isclosures of the specific identities of agents involved in this operation could jeopardize their safety and would effectively eliminate them as law enforcement assets used in electronic surveillance.").

863. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 066 of *2nd Consolidated Exhibits* (Dkt. #821-3) (FBI technical agent memorandum explaining use of portable/transportable wireless device locators and indicating: "Technology Addressed: CDMA").

864. *See Technical Explanations*, Section III(G)(1), *supra* (explaining how the Harris StingRay and KingFish support CDMA, GSM, iDEN, and UMTS wireless technologies but only a maximum of three simultaneously).

865. *See* Maricopa County, FL, USA – **Harris Price List** (Feb 24, 2010), *available at* http://www.maricopa.gov/materials/Awarded_Contracts/PDF/09041-c.pdf (last accessed: Mar. 9,

FBI's devices so that they would be able to send and receive signals to/from the aircard using the CDMA based 1xEV-DO Rel. 0 communications protocol.[866] Once the firmware was loaded onto the FBI's devices, the technical agents were ready to conduct the real-time portion of the aircard locating mission.

27. In preparation of using the Harris StingRay and KingFish to locate the aircard on July 16-17, 2008, the FBI technical agents collected data on all cell sites located in the area identified by FBI Agent Killigrew. In order to complete this task, the FBI used its StingRay in "base station survey" mode[867] while traveling around the area covered by the cell tower range chart/map.[868]

28. While conducting base station surveys, the data collected by the FBI technical agents included signal range estimates for every cell site in the area and radio frequencies used by each cell site sector. The signal range estimates, in combination with other data, were intended to assist the FBI technical agents "in obtaining a start location for the search."[869] The

---

2011), p. 21 (listing "StingRay CDMA Software" part No. "SRAY-CDMA-SW 2" for $22,000.00); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 013 of *2nd Consolidated Exhibits* (Dkt. #821-1) (price list attached).

866. *See Technical Explanations*, Section III(B), *supra* (explaining how all cell sites (including cell site emulators) wishing to communicate with 1xEV-DO Rel. 0 wireless devices must follow the instructions contained in the relevant technical standards).

867. *See Technical Explanations*, Section III(G)(1)(b)(i), *supra* (explaining base station surveys conducted by the Harris StingRay).

868. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 21 of *1st Consolidated Exhibits* (Dkt. #587-2) (cell tower range chart/map).

869. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 066 of *2nd Consolidated Exhibits* (Dkt. #821-3) (FBI technical agent memorandum).

radio frequency information was needed so that the FBI technical agents could properly configure their StingRay and KingFish for use in cell site emulator mode. By referencing a list of all the radio frequencies already in use, the FBI was able to choose an unused frequency for use by its emulated cellular network that would not interfere with the various FCC licensed cellular networks already operating in the noted area.[870]

5. The FBI technical agents had Verizon Wireless reprogram and write data to the aircard so that it would be compatible with the Harris StingRay and KingFish.

29. On July 15, 2008, Verizon Wireless utilized network-initiated Over-The-Air Service Provisioning (OTASP), also known as Over-The-Air Parameter Administration (OTAPA),[871] to surreptitiously write data to the aircard's internal storage device, *i.e.*, the Number Assignment Module (NAM).[872] The purpose of initiating OTAPA was to facilitate compatibility between the aircard, the Verizon Wireless network, and the government's Harris StingRay, KingFish, and related equipment. Verizon Wireless "had a set-up problem with the 'Provisions'"[873] and the government was therefore "not able to get a signal"[874] on July 15th.

870. *See Technical Explanations*, Section III(B)(3)(g)(i), *supra* (explaining how the FCC requires cellular networks to be carefully planned so as to avoid various types of radio signal interference such as interference with ambulance radios).

871. *See Technical Explanations*, Section III(B)(3)(a), *supra* (explaining OTASP and OTAPA).

872. *See Technical Explanations*, Section III(B)(2)(a), *supra* (explaining the Access Terminal NAM).

873. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 26 of *1st Consolidated Exhibits* (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).

874. *Id*.

The following day, all OTAPA issues were resolved and the required data had been written to the aircard's hardware.

30. During the OTAPA session on July 16, 2008, Verizon Wireless wrote data to the aircard consisting of (1) identifying information for the FBI's emulated cell sites,[875] (2) configuration changes that would cause the aircard to recognize the FBI's emulated cell sites as authorized for providing service, and (3) configuration changes that would cause the aircard to attempt connections with the FBI's emulated cell sites prior to attempting connections with actual Verizon Wireless cell sites. The FBI technical agents needed Verizon Wireless to write data to the aircard in this manner because the aircard's properly configured Preferred Roaming List prevented it from accessing rogue, unauthorized cell sites[876][877] such as cell site emulators

875. Cell site emulation was a feature of the Harris StingRay and KingFish used by the FBI technical agents to locate the aircard. *See How The Aircard Was Intruded Upon*, Section IV(B)(9)(a), *supra*.

876. *See Technical Explanations*, Section III(B)(3)(b)(i), *supra* (explaining how an Access Terminal will only scan radio frequencies listed in its Preferred Roaming List Acquisition Table); *id.*, Section III(B)(3)(c)(i), *supra* (explaining how an Access Terminal will only establish a session with an Access Network that has a subnet listed as authorized in the Access Terminal Preferred Roaming List System Table).

877. The only other option for causing the aircard to recognize an emulated cell site as being authorized for service is for the FBI to (1) hijack identifying information for an actual Verizon Wireless cell site by recording Overhead Messages off the air interface, (2) load the Overhead Messages parameters into its cell site emulator, and (3) proceed to spoof an actual Verizon Wireless cell site by broadcasting copies of the hijacked Overhead Messages while within signal range of the aircard. Because the aircard would already have the hijacked identifying information stored on its Preferred Roaming List, the FBI would not need Verizon Wireless to update the list via OTAPA. However, such a spoofing operation would run the risk of intermarket and intramarket radio signal interference causing disruption to numerous users of not only Verizon Wireless' network but also of other cellular and Public Safety Radio Service networks operating in the area. *See id.*, Section III(B)(3)(g)(i), *supra* (explaining interference). In order to avoid spectrum interference, it is a logical assumption that Verizon Wireless updated

used by the FBI.

31. In order to write data to the aircard as described in paragraph No. 30 above, Verizon Wireless: (1) surreptitiously initiated Over-the-Air Parameter Administration (OTAPA) with the aircard over the air interface;[878] (2) disabled the SPL for the aircard's internal NAM by using the aircard's SPC;[879] (3) used the SSD known only to the aircard and Verizon Wireless to validate the aircard's SPASM;[880] (4) transmitted a Configuration Request Message to the aircard instructing it to transmit back all of its stored NAM parameters;[881] (5) received the aircard's transmitted Configuration Response Message containing all of its stored NAM

---

the aircard's Preferred Roaming List with separate frequencies, *etc.* as apposed to the FBI hijacking Overhead Messages from a random Verizon Wireless cell cite for use in a cell site spoofing operation.

Additionally, such a spoofing operation would be a criminal offense. Since October of 1994, it has been a crime for whoever "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver," 18 U.S.C. § 1029(a)(8), meaning "a device or apparatus that can be used to... intercept an... identifier of any telecommunications service, equipment, or instrument," 18 U.S.C. § 1029(e)(8), which would include, *e.g.*, using the StingRay to record the SUBNET_COMMON_LENGTH, SUBNET_COMMON, and other identifying data fields contained in the SectorParameters and QuickConfig messages broadcast by Verizon Wireless cell sites. In the context of 18 U.S.C. § 1029(a)(8), the "intent to defraud" element is satisfied by defrauding a wireless user of service by forcing the wireless device to connect to a spoofed cell site operating outside the wireless carrier network.

878. *See Technical Explanations*, Section III(B)(3)(a), *supra* (explaining how OTAPA is initiated by the wireless carrier surreptitiously).

879. *See id.* (explaining how NAM parameters are protected by the SPC/SPL).

880. *See id.* (explaining how NAM parameters are protected by the SPASM).

881. *See id.* (explaining how the Configuration Request Message is used by the Access Network to read data from the NAM).

parameters;[882] (6) transmitted a Download Request Message[883] to the aircard containing an updated Preferred Roaming List consisting of *(a)* an Acquisition Table containing the band-class and channel number corresponding to the radio frequencies used by FBI's cell site emulators,[884][885] and *(b)* a System Table with the highest priority entry[886] containing the sector subnet and other identifying information for the FBI's cell site emulators;[887] and (7) transmitted a Commit Request Message to the aircard instructing it to write the new Preferred Roaming List to its permanent NAM memory.[888]

32. During the OTAPA session on July 16, 2008, additional data was written to the aircard by Verizon Wireless in order to reprogram the aircard's hardware. Verizon Wireless reprogrammed the aircard to respond in the following manner upon receiving a paging signal

882. *See id.* (explaining how the Configuration Response Message is used to return NAM data to the Access Network).

883. *See id.* (explaining how the Download Request Message is used by the Access Network to write data to the Access Terminal NAM).

884. *See id.*, Section III(B)(3)(b)(i), *supra* (explaining how the Preferred Roaming List Acquisition Table is used to choose radio frequencies to scan for available Access Networks).

885. The frequencies used by the FBI's cell site emulators and loaded onto the aircard by Verizon Wireless were the frequencies chosen after the FBI conducted base station surveys to determine an appropriate unused frequency. *See How The Aircard Was Intruded Upon*, Section IV(B)(4), *supra*.

886. *See Technical Explanations*, Section III(B)(3)(a), *supra* (explaining how Preferred Roaming List System Table entries are listed with the most preferred system first).

887. *See id.,* Section III(B)(3)(c)(i), *supra* (explaining how the Preferred Roaming List System Table is used to identify Access Networks authorized for providing service).

888. *See id.*, Section III(B)(3)(a), *supra* (explaining how the Commit Request Message is used by the Access Network to write the Download Request Message data to the Access Terminal permanent NAM memory).

indicating an incoming 1xRTT voice call: (1) disconnect from its 1xEV-DO Rel. 0 data connection being provided by an actual Verizon Wireless cell site, and (2) enter the Idle State.[889] Additionally, the aircard was reprogrammed to respond to incoming 1xRTT voice calls by generating real-time cell site location information that could be forwarded to the FBI's SF-Martinez DCS-3000 server by Verizon Wireless.[890] Because the aircard is not a telephone[891] and does not normally respond to incoming 1xRTT voice calls,[892] the FBI needed Verizon Wireless to use OTAPA to reprogram the aircard's hardware to respond to the FBI's planned surreptitious voice calls placed to the aircard from a landline telephone.[893][894]

889. *See id.*, Section III(B)(3)(c) *et seq.*, *supra* (explaining the 1xEV-DO Idle State).

890. *See How The Aircard Was Intruded Upon*, Section IV(B)(6), *infra* (explaining the FBI's forced generation of real-time cell site sector location information facilitated through surreptitious voice calls placed to the aircard).

891. *See id.*, Section IV(A), *supra* (general background information on the aircard).

892. *See Technical Explanations*, Section III(B)(3)(g)(ii), *supra* (explaining how non-telephone 1xEV-DO Access Terminals ignore incoming 1xRTT voice calls).

893. *See How The Aircard Was Intruded Upon*, Section IV(B)(8), *infra* (explaining the FBI's denial-of-service attack facilitated through surreptitious voice calls placed to the aircard).

894. In the alternative, if the aircard did not contain adequate manufacturer specific NAM parameters to reprogram the aircard as desired, the FBI had Verizon Wireless use IP Based Over-the-Air Device Management (IOTA-DM) using the Open Mobile Alliance Device Management (OMA DM) protocol to surreptitiously update the aircard's firmware over-the-air so that it would respond to the FBI's planned surreptitious voice calls placed to the aircard from a landline telephone. *See Technical Explanations*, Section III(B)(3)(a), fn. No. 125, *supra* (referencing technical standard explaining protocol used to update wireless device firmware surreptitiously using radio waves). *See also* USDOJ [M.D.La.] Aug. 12, 2008, Response to ACLU FOIA Request No. 07-4130, p. 18 of 42 ("It may also be possible to **flash the firmware of a cell phone**.... You don't even have to have possession of the phone to modify it; **the 'firmware' is modified wirelessly**." (emphasis added)); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 021 of *2nd Consolidated Exhibits* (Dkt. #821-1) (relevant pages of cellfoia_release_074130_20080812.pdf attached with page numbers added).

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

33. In order to write data to the aircard as described in paragraph No. 32 above, Verizon Wireless: (1) surreptitiously initiated Over-the-Air Parameter Administration (OTAPA) with the aircard over the air interface;[895] (2) disabled the SPL for the aircard's internal NAM by using the aircard's SPC;[896] (3) used the SSD known only to the aircard and Verizon Wireless to validate the aircard's SPASM;[897] (4) transmitted a Configuration Request Message to the aircard instructing it to transmit back all of its stored NAM parameters;[898] (5) received the aircard's transmitted Configuration Response Message containing all of its stored NAM parameters;[899] (6) transmitted a Download Request Message[900] to the aircard containing manufacturer-specific NAM parameters[901] instructing the aircard to *(a)* generate real-time cell site location information upon receiving an incoming 1xRTT paging signal, and *(b)* disconnect from its Verizon Wireless 1xEV-DO Rel. 0 data connection upon receiving an incoming 1xRTT paging signal; and (7) transmitted a Commit Request Message to the aircard instructing it to

895. *See Technical Explanations*, Section III(B)(3)(a), *supra* (explaining how OTAPA is initiated by the wireless carrier surreptitiously).

896. *See id.* (explaining how NAM parameters are protected by the SPC/SPL).

897. *See id.* (explaining how NAM parameters are protected by the SPASM).

898. *See id.* (explaining how the Configuration Request Message is used by the Access Network to read data from the NAM).

899. *See id.* (explaining how the Configuration Response Message is used to return NAM data to the Access Network).

900. *See id.* (explaining how the Download Request Message is used by the Access Network to write data to the Access Terminal NAM).

901. *See id.* (explaining how an Access Terminal NAM contains manufacturer-specific NAM parameters).

write the new manufacturer-specific NAM parameters to permanent NAM memory.[902]

6. The FBI used the SF-Martinez DCS-3000 Pen/Trap device to obtain real-time cell site sector location information to narrow the geographical area of where to use the StingRay, KingFish, and related equipment.

34. Prior to using the Harris StingRay, KingFish, and related equipment to pinpoint the precise location of the aircard and its user, the FBI needed to first narrow the geographical area of where to search for the aircard. In order to accomplish this task, the three FBI technical agents planned to use real-time cell site sector location information to determine the Verizon Wireless cell site sector providing service to the aircard.[903] In order to obtain the needed real-time cell site sector location information relating to the aircard, the FBI relied upon the N.D.Cal. 08-90331MISC-RS order[904] to use a Pen/Trap device.

35. At the time of the aircard locating mission, Verizon Wireless had not yet configured its network Intercept Access Points (IAPs)[905] to provide FBI DCS-3000 servers[906]

902. *See id.* (explaining how the Commit Request Message is used by the Access Network to write the Download Request Message data to the Access Terminal permanent NAM memory).

903. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 069 of *2nd Consolidated Exhibits* (Dkt. #821-4) (June 7, 2011 letter from AUSA Battista to the defendant, p. 1: AUSA Battista indicating that the FBI technical agents "generate[d] activity on the device [(*i.e.*, aircard)] in order to obtain the cell site serving the device pursuant to the [N.D.Cal 08-90331MISC-RS] Court Order...").

904. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Materials Related To Applications And Court Orders Numbered 08-90330 And 08-90331, Authorized By Magistrate Judge Richard Seeborg, Northern District Of California, On July 11, 2008* (Dkt. #470-2).

905. *See Technical Explanations*, Section III(H)(2) and fn. No. 657, *supra* (explaining Intercept Access Points).

906. *See Technical Explanations*, Section III(H)(4), *supra* (explaining DCS-3000 servers, *i.e.*,

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

(Pen/Trap devices) with real-time cell site location information relating to 1xEV-DO Rel. 0 data connections for aircards.[907] As a workaround, the FBI decided to "ping the number associated to the [air]card..."[908] in order to generate the needed data. By pinging the aircard (*i.e.*, placing surreptitious telephone calls to the aircard without having it ring or answer),[909][910] the FBI would force the aircard to generate real-time cell site sector location information associated with a 1xRTT voice call (as apposed to an 1xEV-DO Rel. 0 data connection) that could be forwarded to the FBI SF-Martinez DCS-3000 server from a Verizon Wireless IAP.[911]

Pen/Trap devices and the FBI Digital Collection Program).

907. *See, e.g.,* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 27 of *1st Consolidated Exhibits* (Dkt. #587-2) (FBI Agent Murray's rough notes indicating that no cell site data is available for an aircard when using a Pen/Trap device); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 28 of *1st Consolidated Exhibits* (Dkt. #587-2) (June 27, 2008 email from FBI Agent Murray to FBI Agent Leising: "Verizon Wireless can't separate tower data from content for a broadband card.").

908. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 26 of *1st Consolidated Exhibits* (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 27 of *1st Consolidated Exhibits* (Dkt. #587-2) (FBI Agent Murray's rough notes indicating that "you have to call into the card.").

909. *See How The Aircard Was Intruded Upon*, Section IV(A)(1), *supra* (explaining how the aircard is incapable of ringing or answering calls).

910. The only other option for the government was to obtain a Title III wiretap warrant to receive real-time cell site location information along with the communications content of which the location data could not be separated. *See*, *e.g.*, United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 26 of *1st Consolidated Exhibits* (Dkt. #587-2) (Based on the destination IP addresses obtained via subpoenas, the government was "in the process of securing a Title 3" so that agents could "monitor the content of the computer that the [air]card [][was] being used [][with]" in order to "possibly triangulate the signal.")

911. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 072 of *2nd Consolidated Exhibits* (Dkt. #821-4) (December 9, 2011 letter from AUSA Battista to the defendant, p. 1: AUSA Battista indicating that "the incoming phone calls made to your aircard

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

36. Beginning at 11:02am on July 16, 2008,[912] the FBI began to place surreptitious telephone calls to the aircard using the public telephone network[913] while Verizon Wireless, acting pursuant to the N.D.Cal. 08-90331MISC-RS order, forwarded the resulting LAESP messages[914] (*i.e.*, Pen/Trap data including the cell site and sector accessed by the aircard) to the FBI SF-Martinez DCS-3000 server in real-time.[915] The FBI continued to surreptitiously call the aircard a total of 32 times until 5:03pm on July 16, 2008.[916] The LAESP messages sent over that six hour period informed the FBI that the aircard was located within the signal coverage area of sector No. 3, Verizon Wireless cell site No. 5, having a latitude of 37.369733 and longitude of -121.923442 with a cell site street address of 2001 Gateway Place, San Jose,

---

were placed in order to stimulate your aircard to provide the identity of the cell tower with which your aircard connected during these calls.").

912. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 06 of *1st Consolidated Exhibits* (Dkt. #587-1) (LAESP messages sent to the SF-Martinez DCS-3000 server (Pen/Trap device) by Verizon Wireless IAPs); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 07, EXHIBIT 08, EXHIBIT 09, and EXHIBIT 10 of *1st Consolidated Exhibits* (Dkt. #587-1) (The FBI's "human readable" CDNRS files created from the Verizon Wireless LAESP messages).

913. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 069 of *2nd Consolidated Exhibits* (Dkt. #821-4) (June 7, 2011 letter from AUSA Battista to the defendant, p. 1: "The operators called this number [belonging to the aircard] using the Public Switched Telephone Network to generate activity on the device in order to obtain the cell site serving the device...").

914. *See Technical Explanations*, Section III(H)(3), *supra* (explaining LAESP messages).

915. *See id.* (neither LAESP messages, call-identifying information, nor Pen/Trap data are amongst the data recorded and retained by Verizon Wireless).

916. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 07, EXHIBIT 08, EXHIBIT 09, and EXHIBIT 10 of *1st Consolidated Exhibits* (Dkt. #587-1) (The FBI's "human readable" CDNRS files created from the Verizon Wireless LAESP messages).

CA 95110.[917]

37. While the FBI called/pinged the aircard, the real-time cell site sector location information was fed into the SF-Martinez DCS-1020 gateway server[918] and sent over the Internet via a Virtual Private Network (VPN) to a wireless cellular modem[919] (*i.e.*, the FBI's own aircard) paired with a laptop computer being accessed by the FBI technical agents while they were lurking the streets of Santa Clara, CA looking for the aircard.[920] The FBI technical agents used the real-time cell site sector location information to narrow the geographical area of where to use the Harris StingRay, KingFish, and related surveillance equipment to search for the aircard.[921]

38. Considering the aircard is not a telephone and does not have telephone service,

917. *See id.* (showing a "location = 5-3" relating to the FBI's surreptitious phone calls); *see also How The Aircard Was Intruded Upon*, Section IV(B)(2), *supra* (listing location information for Verizon Wireless cell site No. 5 in San Jose, CA).

918. *See Technical Explanations*, Section III(H)(8), *supra* (explaining DCS-1020 gateway servers).

919. *See id*.

920. Using a DCS-1020 gateway server, VPN, and aircard is the standard Digital Collection Program (DCS) operation conducted by FBI Wireless Intercept and Tacking Team (WITT) agents to locate wireless devices. *See Technical Explanations*, Section III(H) *et seq.*, *supra* (explaining the FBI Digital Collection Program). The FBI's WITT was used to locate my aircard. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 066 of *2nd Consolidated Exhibits* (Dkt. #821-4) (FBI technical agent memorandum stating: "Personnel Performing Mission: TTA-WITT").

921. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 068 of *2nd Consolidated Exhibits* (Dkt. #821-3) (May 2, 2011 letter from AUSA Battista to the defendant, p. 5: FBI Agent Killigrew advised FBI Agent Murray that "when a call comes into the monitoring device, it produces a shadow over the sector of the tower the phone is hitting.").

[922] the FBI's surreptitious phone calls did not cause the aircard to "ring" and otherwise did not cause the aircard to notify the aircard user that the FBI was calling the aircard. As shown by the LAESP messages[923] and as admitted by the prosecution,[924] the FBI's surreptitious phone calls were not answered by the aircard in any fashion, *i.e.*, no calls were ever established as "in progress" and the aircard was never "off the hook."

39. As supported by sources cited in the *Technical Explanations*, Section III(H)(3), *supra*, and as admitted by the prosecution,[925] Verizon Wireless only buffered the aircard's Pen/Trap data and neither recorded nor stored the data prior to forwarding it to the FBI. Even if Verizon Wireless, through a separate mechanism, simultaneously recorded *some* of the data

922. *See How The Aircard Was Intruded Upon*, Section IV(A)(1), *supra* (general background information on the aircard).

923. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 06 of *1st Consolidated Exhibits* (Dkt. #587-1) (LAESP messages showing that the FBI's surreptitious phone calls were forwarded to internal Verizon Wireless telephone numbers set up to handle unanswered calls).

924. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 069 of *2nd Consolidated Exhibits* (Dkt. #821-4) (June 7, 2011 letter from AUSA Battista to the defendant, p. 1: "The forwarded numbers arose after the operators of the equipment used to locate the aircard called a telephone number associated with the aircard.... Because the aircard device was not a conventional telephone, incoming calls to the device could not be connected to it as a normal call. The incoming calls in question were forwarded by the Verizon Wireless network to the various numbers which belong to, and are used by, Verizon Wireless for processing incoming calls that cannot be connected/terminated to the original called number - *i.e.*, the targeted number.").

925. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 067 of *2nd Consolidated Exhibits* (Dkt. #821-3) (January 28, 2011 letter from AUSA Battista to the defendant, p. 4: "Any information transmitted to the FBI pursuant to any disclosed court Order was received by Verizon Wireless, buffered by Verizon Wireless and then transmitted to the FBI. The time period from receipt by Verizon Wireless, buffering and then transmission to the FBI is extremely short.").

sent in the real-time LAESP messages (for example, recording "call-detail records" as historical data via separate network elements), it still did not record cell site **sector** information before sending it to the FBI. The data retention chart showing Verizon Wireless' practices for recording historical data lists "Cell towers used by phone" but not cell site sectors.[926] Additionally, an analysis of the aircard's historical cell site information recorded by Verizon Wireless[927] confirms that it only recorded and saved cell site locations—not the more precise cell site **sectors** as was provided in real-time via the LAESP messages sent to the FBI.

7. The FBI obtained additional real-time aircard data from Verizon Wireless through means other than the SF-Martinez DCS-3000 Pen/Trap device.

40. As explained above, the FBI relied upon the N.D.Cal. 08-90331MISC-RS order and used the SF-Martinez DCS-3000 server (Pen/Trap device) to obtain real-time cell site **sector** location information corresponding to the location of the aircard. In order to further narrow the location of where to use the Harris StingRay, KingFish, and related equipment, the FBI also sought further real-time aircard data from Verizon Wireless while relying upon the N.D.Cal. 08-90330MISC-RS order. Because the government destroyed and/or failed to

926. *See* Department of Justice, *Retention Periods of Major Cellular Service Providers* (Aug. 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf (last accessed: Dec. 7, 2011); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 054 of *2nd Consolidated Exhibits* (Dkt. #821-3) (data retention period chart attached).

927. *See* aircard historical cell site information records provided to the FBI by Verizon Wireless: United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 02 of *1st Consolidated Exhibits* (Dkt. #587-1); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 03 of *1st Consolidated Exhibits* (Dkt. #587-1); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 05 of *1st Consolidated Exhibits* (Dkt. #587-1).

preserve all data seized from Verizon Wireless,[928] the precise and full nature of the data and how it was obtained and/or generated is unknown. However, at the very least, an FBI technical agent received from Verizon Wireless the aircard's distance from a specific cell site sector.[929]

8. The FBI's surreptitious phone calls booted the aircard off the Internet so that the FBI's StingRay and related equipment could hijack the aircard's signal from Verizon Wireless.

41. Prior to conducting geolocation techniques using the Harris StingRay and KingFish, the FBI first needed to force the aircard to establish a session[930] with the FBI's emulated cellular network. Due to technical limitations of the 1xEV-DO Rel. 0 communications protocol, the Harris StingRay and KingFish were incapable of forcing the aircard to handoff an open data connection established with a Verizon Wireless cell site to the FBI's emulated cellular network.[931] The only possible inter-system handoffs in 1xEV-DO Rel.

928. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court Order* (Dkt. #723, p. 14) (Noting the settled fact that "[a]ll data generated by the [] [portable/transportable wireless device locators] and received from Verizon as part of the locating mission was destroyed by the government shortly after Defendant's arrest on August 3, 2008.").

929. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 066 of *2nd Consolidated Exhibits* (Dkt. #821-3) (FBI technical agent memorandum stating that "Verizon gave a distance from the tower to the target.")

930. *See Technical Explanations*, Section III(B)(3)(c)(iii), *supra* (explaining 1xEV-DO Rel. 0 sessions).

931. As explained in the *Technical Explanations*, Section III(B)(3)(d) *et seq.*, *supra*, 1xEV-DO Rel. 0 Access Networks (which include the FBI's cell site emulators) are incapable of accepting a wireless device **active connection** "handoff" from another Access Network without significant collaboration between the Access Terminal, the serving Access Network, the new Access Network, and the underlying network. Because the FBI's emulated cell sites are on their own network not connected to Verizon Wireless, the only type of aircard handoff possible is an Idle State handoff, which is done autonomously by the aircard. *See id*.

0 are Idle State Route Updates[932] and the Harris products are not immune to this inherent protocol limitation.[933]

42. Because there were attempts to keep the aircard continuously in the Connected State[934] (*i.e.*, connected to the Internet) whenever powered on,[935] the FBI technical agents first had to knock the aircard offline and into the Idle State[936] so that it would be in a position to conduct an Idle State Route Update (*i.e.*, handoff)[937] of its signal to the FBI's emulated cellular network. With the aircard in the Idle State, the FBI's emulated cellular network would have the opportunity to broadcast a very strong signal and present itself to the aircard as an available and preferred network over all Verizon Wireless cell sites in the area.[938]

---

932. *See Technical Explanations*, Section III(B)(3)(d) *et seq.*, *supra* (explaining the different types of handoffs dictated by the Default Route Update Protocol).

933. *See Technical Explanations*, Section III(B)(3), *supra* (explaining how all 1xEV-DO Rel. 0 compatible Access Terminals and Access Networks must follow the instructions contained in the relevant standards).

934. *See Technical Explanations*, Section III(B)(3)(c)(vi), *supra* (explaining technical procedures for opening a 1xEV-DO Rel. 0 connection).

935. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection* (Dkt. #824-3, ¶ 17-20, p. 6-7).

936. "It must be ensured, that the mobile phone of the observed person is in standby mode and the correct network operator is found out. Otherwise, for the Mobile Station, there is no need to log into the simulated Base Station." Strobel, Daehyun, *IMSI Catcher*, Ruhr-Universit¨at Bochum, Jul. 13, 2007, *available at* http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf (last accessed: Feb. 10, 2012), p. 16 (PDF, p. 20).

937. *See Technical Explanations*, Section III(B)(3)(d)(i), *supra* (explaining 1xEV-DO Rel. 0 Idle State Route Updates).

938. As explained in *How The Aircard Was Intruded Upon*, Section IV(B)(5), *supra*, the FBI previously had Verizon Wireless use OTAPA to update the aircard's Preferred Roaming List

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

43. As explained by the FBI, in addition to generating real-time cell site sector location information, the previously noted surreptitious phone calls[939] also served the purpose of knocking the aircard offline from its Verizon Wireless data connection so that it would "connect to the best available cell phone tower that will provide it service."[940] Each surreptitious voice call placed to the aircard by the FBI resulted in Verizon Wireless sending a paging signal from sector No. 3, cell site No. 5, notifying the aircard of the incoming call.[941] Based on the aircard's new NAM parameter configuration facilitated via OTAPA,[942] the paging signals caused the aircard to disconnect from its Verizon Wireless 1xEV-DO Rel. 0 data connection and enter the Idle State.

44. While in the Idle State, the aircard had the opportunity to use the Default Route Update Protocol to decide whether to conduct an Idle State Route Update (*i.e.*, handoff) to a cell site broadcasting a pilot signal with a higher signal strength than the current serving cell

with identifying information on the FBI's cell site emulators.

939. *See How The Aircard Was Intruded Upon*, Section IV(B)(6), *supra* (explaining details on the FBI's surreptitious phone calls placed to the aircard).

940. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 071 of *2nd Consolidated Exhibits* (Dkt. #821-4) (December 2, 2011 letter from AUSA Battista to the defendant, p. 1).

941. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 07, EXHIBIT 08, EXHIBIT 09, and EXHIBIT 10 of *1st Consolidated Exhibits* (Dkt. #587-1) (The FBI's "human readable" CDNRS files created from the Verizon Wireless LAESP messages showing a "location = 5-3" relating to the FBI's surreptitious phone calls).

942. *See How The Aircard Was Intruded Upon*, Section IV(B)(5), *supra* (explaining how the aircard was reprogrammed using OTAPA).

site sector.[943] After each surreptitious voice call placed to the aircard (over the previously noted six (6) hour period), the FBI technical agents used their StingRay in the area of the cell tower range chart/map to broadcast an emulated cellular network signal in hopes that the aircard would detect the network and conduct an Idle State Route Update (*i.e.*, handoff) to the StingRay.

45. Because their were attempts to keep the aircard continuously connected to the Internet,[944] the FBI had a very short window of time to force the aircard to handoff its signal to the StingRay after each surreptitious voice call. Due to the auto-reconnect software,[945] and/or typical manual reconnect attempts,[946] the FBI needed to repeatedly call the aircard in order to repeatedly boot it offline over the six hours of surreptitious phone calls. Each few minute window of time that followed each denial-of-service attack (*i.e.*, surreptitious phone call) was used by the FBI to move its StingRay, while in cell site emulator mode, to various positions until it was close enough to the aircard to force an Idle State Route Update (*i.e.*, handoff).

943. *See Technical Explanations*, Section III(B)(3)(d)(i), *supra* (explaining 1xEV-DO Rel. 0 Idle State Route Updates).

944. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection* (Dkt. #824-3, ¶ 17-20, p. 6-7).

945. *See id*.

946. *See id*.

9. The FBI technical agents used the Harris StingRay, KingFish, and related equipment to locate the aircard precisely inside apartment No. 1122.

a. Cell site emulation and forced connection handoff.

46. During the final surreptitious phone call placed to the aircard at 5:03pm on July 16, 2008, the FBI technical agents finally positioned their StingRay close enough to the aircard and to force it to acquire the pilot signal[947] of the FBI's emulated cellular network. Because the StingRay was broadcasting a stronger pilot signal than the legitimate Verizon Wireless cell sites in the area, the aircard began an Idle State Route Update (*i.e.*, handoff) of its Verizon Wireless connection to the StingRay.[948] Once the Idle State Route Update was in progress, the aircard was no longer communicating with Verizon Wireless and was now forced unwittingly to communicate directly with the government.

47. While the aircard was in direct communication with the government, the FBI technical agents engaged in a series of actions that further intruded upon the aircard user's privacy, property, and possessory interests. The proceeding subsections detail the specific actions carried out by the FBI technical agents after the aircard acquired the StingRay's pilot signal. All of the government actions explained below were necessary in order for the FBI technical agents to locate the aircard.

947. *See Technical Explanations*, Section III(B)(3)(b)(ii), *supra* (explaining 1xEV-DO Rel. 0 Access Terminal Pilot Acquisition Substate).

948. Although an archaic technical term, Harris refers to this technique as "forced registration." *See id.*, Section III(G)(b)(iii), *supra*; *see also id.*, Section III(B)(3)(c)(iii) and II(B)(3)(d), *supra* (explaining how in the context of 1xEV-DO Rel. 0 and other all IP based cellular networks, wireless devices establish "sessions" and conduct "route updates" with cell sites as apposed to "registering" with cell sites).

b. The FBI repeatedly wrote data to the aircard using its StingRay.

48. Once the Idle State Route Update was complete, the aircard began monitoring the StingRay's broadcast Control Channel as dictated by 1xEV-DO Rel. 0 technical standards.[949] Via its forward link Control Channel, the StingRay sent a Sync message to the aircard with the following data fields intended to be written to the aircard's internal storage: (1) MessageID, (2) MaximumRevision, (3) MinimumRevision, (4) PilotPN, and (5) SystemTime.[950] Upon receiving the Sync message, the data contained in the message was written to the aircard's internal storage so that the aircard could further communicate with the StingRay.[951]

49. Once the data contained in the Sync message had been written to the aircard's internal storage, the aircard began to monitor the StingRay's overhead messages broadcast over its Control Channel as dictated by 1xEV-DO Rel. 0 technical standards.[952] The aircard received the StingRay's overhead messages which included the QuickConfig message and SectorParameters message.[953] The QuickConfig message contained numerous data fields including MessageID, ColorCode, SectorID24, SectorSignature, AccessSignature, Redirect, RPCCount, ForwardTrafficValid, and a Reserved field.[954] The SectorParameters message contained numerous data fields including MessageID, CountryCode, SectorID, SubnetMask,

949. *See Technical Explanations*, Section III(B)(3)(b)(iii), *supra*.

950. *See id*.

951. *See id*.

952. *See id.*, Section III(B)(3)(c)(i), *supra*.

953. *See id*.

954. *See id*.

SectorSignature, Latitude, Longitude, RouteUpdateRadius, LeapSeconds, LocalTimeOffset, ReverseLinkSilenceDuration, ReverseLinkSilencePeriod, ChannelCount, Channel, NeighborCount, NeighborPilotPN, NeighborChannelIncluded, NeighborChannel, NeighborSearchWindowSizeIncluded, NeighborSearchWindowSize, NeighborSearchWindowOffsetIncluded, NieghborSearchWindowOffset, and a Reserved field. [955] Upon receiving the overhead messages, the data contained in the messages was written to the aircard's internal storage so that the aircard could further communicate with the StingRay. [956]

50. Immediately after receiving the SectorParameters message, the aircard used the SectorID and SubnetMask data fields to determine the subnet of the system to which the StingRay belonged.[957] After deducing the StingRay's subnet, the aircard checked its locally stored Preferred Roaming List System Table to determine if the subnet was listed as corresponding to a group of Access Networks (*i.e.*, a system) authorized for providing wireless service.[958] Because the government had Verizon Wireless update the aircard's Preferred Roaming List, the aircard found the StingRay's subnet listed as an authorized network and believed that it was accessing a legitimate Verizon Wireless cell site and not a StingRay in cell site emulator mode.

955. *See id*.
956. *See id*.
957. *See id*.
958. *See id*.

51. Prior to beginning the Access Probe process to establish a session with the FBI's StingRay, the aircard received the StingRay's AccessParameters message broadcast by the StingRay.[959] The AccessParameters message contained numerous data fields including MessageID, AccessCycleDuration, AccessSignature, OpenLoopAdjust, ProbeInitialAdjust, ProbeNumStep, PowerStep, PreambleLength, CapsuleLengthMax, Apersistence, and a Reserved field.[960] Upon receiving the AccessParameters message, the data contained in the message was written to the aircard's internal storage so that the aircard could further communicate with the StingRay via the Access Probe process.[961][962]

c. The StingRay deactivated 1xEV-DO Rel. 0 security layer encryption during session establishment causing the aircard's signals to be transmitted in plaintext and exposed to third-parties.

52. While the aircard was establishing a session[963] during the Access Probe process, the FBI's StingRay failed to initiate negotiation of the security layer protocols resulting in no session key being created for use in data integrity, authentication, and encryption in the MAC

959. *See id.*, Section III(B)(3)(c)(ii), *supra*.

960. *See id*.

961. *See id*.

962. After the Access Probe process, there are numerous other occurrences of an Access Network (*e.g.*, the StingRay) writing data to an Access Terminal (*e.g.*, the aircard). For example, the UATIAssignment message. *See Technical Explanations*, Section III(B)(3)(c)(iii), *supra*. Not all occurrences of the StingRay writing data to the aircard are explained in this declaration.

963. *See Technical Explanations*, Section III(B)(3)(c)(iii), *supra* (explaining 1xEV-DO Rel. 0 session establishment).

layer.[964] The prosecution admitted that no encryption was in use while the FBI's surveillance equipment was communicating with the aircard.[965] Because the FBI failed to implement standard security layer encryption over the air interface, the aircard's signals containing private information (*e.g.*, the ESN via the HardwareIDRequest message) and geolocation information were exposed to third-parties over the air interface.

d. The FBI used its StingRay to download data stored on the aircard's internal storage device (*i.e.*, the aircard's Electronic Serial Number (ESN)).

53. After the aircard and the FBI's StingRay had established a session, the StingRay was only aware that a 1xEV-DO Rel. 0 compatible wireless device had connected to its emulated cellular network while the identity of the device remained unknown.[966] Prior to conducting geolocation techniques, the FBI technical agents needed to determine if the wireless device connecting to its emulated cellular network was actually the aircard and not another device. In order to identify the aircard prior to collecting signals for triangulation purposes, the

964. *See id.*, Section III(B)(3)(c)(iv), *supra* (explaining how the Access Terminal is responsible for initiating security layer encryption in 1xEV-DO Rel. 0).

965. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 072 of *2nd Consolidated Exhibits* (Dkt. #821-4) (December 9, 2011 letter from AUSA Battista to the defendant, p. 1: AUSA Battista indicating that "while the specific techniques used to locate the aircard are Law Enforcement Sensitive, neither encryption nor encryption-defeating techniques were used in this location mission.").

966. *See Technical Explanations*, Section III(B)(3)(c)(v), *supra* (explaining how prior to sending the HardwareIDRequest message, the Access Network does not have the absolute identity of the Access Terminal).

StingRay sent a HardwareIDRequest message[967][968] (via radio wave transmissions) to the receive antenna of what was then an unknown device. The aircard, being the unknown device, responded by transmitting back its ESN to the FBI's StingRay via a HardwareIDResponse message.[969] The FBI technical agents logged (*i.e.*, seized) the ESN it received directly from the aircard and then compared it to the aircard ESN it previously received from Verizon Wireless via subpoena.[970] By matching the two separate ESNs, the FBI technical agents determined that its StingRay was communicating with the right wireless device.

e. The FBI used the StingRay to send location finding interrogation signals into apartment No. 1122 and into the aircard in order to search out the location of the aircard and its user.

54. Once the FBI downloaded the aircard's stored ESN via the HardwareIDRequest message, the FBI technical agents knew that they had locked-on to the right wireless device and began "using [][the] 'Stingray' to pinpoint the location of the aircard."[971] The StingRay conducts geolocation through the process of interrogation involving the transmission of

967. *See id*.

968. *See id.*, Section III(G)(1)(a)(iv), *supra* (explaining how the Harris StingRay downloads identifying data from wireless devices such as ESNs).

969. *See id.*, Section III(B)(3)(c)(v), *supra*.

970. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Submission Of Documents Related To District Of Arizona Grand Jury Subpoenas 07-03-609 And 07-03-615 Obtained To Facilitate Locating The Aircard* (Dkt. #565-1).

971. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 26 of *1st Consolidated Exhibits* (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).

specially crafted location finding interrogation signals sent to a target wireless device.[972] In response to the location finding interrogation signals, the target wireless device responds with location finding response signals.[973] The prosecution conceded that the FBI technical agents used interrogation to locate the aircard and it user within apartment No. 1122.[974] Because the aircard was located inside apartment No. 1122, the StingRay's location finding interrogation signals penetrated the exterior walls of the apartment and entered the confines of apartment No. 1122. Once inside the confines of apartment No. 1122, the StingRay's location finding interrogation signals searched out the aircard, entered the aircard's receive antenna, and forced the aircard to transmit location finding response signals telling of its location.[975]

55. While using the StingRay, the FBI technical agents used the AmberJack phased array beam-forming antenna to transmit a highly directional and concentrated beam of location finding interrogation signals into apartment No. 1122.[976] The AmberJack antenna is different from cell site antennas in the effect that it is capable of facilitating highly precise angle-of-

---

972. *See Technical Explanations*, Section III(G)(1)(b)(iv), *supra* (explaining the interrogation techniques used by the Harris StingRay to locate wireless devices).

973. *See id*.

974. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Government's Response To Motion For Discovery* (Dkt. #602, p. 3) ("The equipment mimicked a Verizon Wireless cell tower and sent and received signals directly to and from the aircard."); United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court Order* (Dkt. #723, p. 14) (signals sent by the surveillance equipment used by the FBI technical agents were "signals that would not have been sent to the aircard in the normal course of Verizon's operation of its cell towers.").

975. *See Technical Explanations*, Section III(G)(1)(a)(v), *supra* (explaining the interrogation techniques used by the StingRay and KingFish to locate wireless devices).

arrival measurements in order to obtain a line-bearing to a target wireless device.[977]

f. The FBI collected the aircard's signal transmissions sent in response to the location finding interrogation signals sent to the aircard by the FBI via the StingRay.

56. While the FBI technical agents were conducting interrogation, they used the StingRay to collect (*i.e.*, seize) the aircard's location finding response signals.[978] During the September 22, 2011 court hearing, the prosecution admitted that the aircard's signals were seized by the FBI with its concession that the "device sent signals to, and **received signals from**, the air card[.]"[979] The signals that were seized contained information (*i.e.*, the UATI assigned to the aircard by the StingRay during session establishment)[980] allowing the FBI to determine that the signals were being transmitted by the aircard. The signals in question were generated and transmitted by the aircard upon the StingRay's specific instruction (via the location finding interrogation signals) and would not have been transmitted during the aircard's communications with actual Verizon Wireless cell sites.

976. *See id.*, Section III(G)(1)(a)(iii), *supra* (explaining the AmberJack phased array antenna used with the StingRay to locate wireless devices).

977. *See id*.

978. *See id*.

979. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *October 5, 2011 Court Order* (Dkt. #644, p. 2) (emphasis added) (noting undisputed facts).

980. *See Technical Explanations*, Section III(B)(3)(c)(iii), *supra* (explaining how the Access Terminal UATI is assigned by the Access Network and used by the MAC layer protocol to label and identify transmissions during a session).

g. In order to determine the location of the aircard and its user, the FBI conducted triangulation techniques on the aircard's location finding response signals collected by the StingRay.

57. While conducting interrogation techniques, the FBI technical agents engaged in active approach to facilitate triangulation of the aircard's collected location finding response signals. The approach method involves using the StingRay to collect and measure location finding response signals while emulating a cell site at one location and then repeatedly moving the StingRay to new locations to repeat cell site emulation, signal collection, and signal measurements.[981] By emulating a cell site at numerous locations, enough geolocation measurements can be taken by the StingRay to triangulate the location of a wireless device.[982] The prosecution admitted that the StingRay was used to triangulate the location of the aircard in this manner when it conceded that the FBI technical agents "would take a reading, move to a new location, take another reading, move to another location, *etc.*"[983]

58. While conducting interrogation techniques during movement of the StingRay in the geographical area surrounding the aircard (*i.e.*, active approach), the FBI technical agents conducted numerous geolocation measurements on collected aircard signals. The geolocation

981. *See id.*, Section III(G)(1)(b)(v), *supra* (explaining the approach method used by the StingRay and KingFish to locate wireless devices).

982. *See id*.

983. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court Order* (Dkt. #723, p. 14) (noting government concession).

measurement techniques included time-of-flight,[984] power-distance,[985] angle-of-arrival,[986] statistical functions,[987] and data fusion.[988] The geolocation measurement techniques used by the FBI technical agents meet the definition of triangulation in the geolocation context.[989]

59. At some point prior to 4:45pm on July 16, 2008, the FBI technical agents were able to triangulate the location of the aircard and its user as being somewhere within a smaller geographical area including the Domicilio apartment complex. In a report of investigation, USPIS Inspector Wilson indicated that at some point after July 16, 2008 he was informed that the FBI technical agents "were able to get a positive signal at an apartment complex in Santa Clara[,]" *i.e.*, the Domicilio apartment complex located at 431 El Camino Real, Santa Clara, CA 95050.[990] At approximately 4:45pm on July 16, 2008, government agents began visual

984. *See Technical Explanations*, Section III(G)(1)(a)(i), *supra* (explaining TOF as used by the StingRay and KingFish to locate wireless devices).

985. *See id.*, Section III(G)(1)(a)(ii), *supra* (explaining power-distance as used by the StingRay and KingFish to locate wireless devices).

986. *See id.*, Section III(G)(1)(a)(iii), *supra* (explaining AOA as used by the StingRay and KingFish to locate wireless devices).

987. *See id.*, Section III(G)(1)(a)(iv), *supra* (explaining statistical functions as used by the StingRay and KingFish to locate wireless devices).

988. *See id.*, Section III(G)(1)(a)(v), *supra* (explaining data fusion as used by the StingRay and KingFish to locate wireless devices).

989. *See id.*, Section III(C), *supra* (explaining triangulation in the context of geolocation of radio frequency (RF) signals).

990. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 26 of *1st Consolidated Exhibits* (Dkt. #587-2) (August 7, 2008 USPIS Investigation Details Report entry by USPIS Inspector Wilson).

surveillance of the Domicilio apartment complex.[991] Therefore, it can be reasonably assumed that the FBI technical agents used their StingRay and related equipment to narrow down the location of the aircard and its user to a smaller geographical area, which included the Domicilio apartment complex, shortly before 4:45pm on July 16, 2008.

h. The FBI technical agents used the KingFish within the Domicilio apartment complex to pinpoint the exact location of the aircard and its user within apartment No. 1122.

60. In Section IV(A)(2) *et seq.*, *supra*, it was explained how relevant evidence, heuristics, and process of elimination confirm that the handheld equipment used by the FBI technical agents included the Harris KingFish. The KingFish operates nearly identical to the StingRay with the only relevant difference being that it is a man-portable wireless device locator, as apposed to a vehicle-transportable wireless device locator, and is capable of locating wireless devices more accurately than the StingRay.[992] Therefore, all of the operations explained in Sections III(B)(9)(a) through (g), *supra* (paragraph Nos. 46-59 above), were repeated by the FBI technical agents while it used the handheld KingFish within the Domicilio apartment complex.

61. Once the FBI technical agents narrowed the location of the aircard and its user to a smaller geographical area including the Domicilio apartment complex, they began "to pin the

991. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 097 of *2nd Consolidated Exhibits* (Dkt. #821-6) (surveillance log indicating that visual surveillance of the Domicilio apartment complex began at 4:45pm on July 16, 2008).

992. *See Technical Explanations*, Section III(G)(1) *et seq.*, *supra*.

exact number"[993] where the aircard was located. In order to do so, "the FBI used handheld equipment from within the Domicilio apartment complex[,]"[994] *i.e.*, the Harris KingFish.[995] At approximately 12:53am on July 17, 2008, FBI Agent Murray sent a text message to FBI Agent Killigrew stating that "[w]e are down to an apt complex[.]"[996] At approximately 2:42am on July 17, 2008, one of the FBI technical agents locating the aircard sent a text message to an unknown individual stating that they had "[f]ound the card[]" and "Sqd is working on a plan for arrest[.]"[997] Additionally, the prosecution agreed "to allow the Court to

993. *See id*.

994. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Government's Response To Motion For Discovery* (Dkt. #602, p. 3); *see also* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *October 5, 2011 Court Order* (Dkt. #644, p. 2) (Establishing as undisputed that the surveillance equipment "used to locate the air card in this case was used by government agents on foot and within the Domicilio apartment complex[.]").

995. The FBI technical agents destroyed all real-time geolocation data and other data collected by the StingRay and KingFish approximately 18 days after the aircard was located. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court Order* (Dkt. #723, p. 14) (Noting the settled fact that "[a]ll data generated by the [] [portable/transportable wireless device locators] and received from Verizon as part of the locating mission was destroyed by the government shortly after Defendant's arrest on August 3, 2008."). Because geolocation evidence was destroyed, the precise geographical and temporal point at which the FBI technical agents stopped using the StingRay and started using the KingFish in unknown. It is known, however, that the StingRay first narrowed the location of the aircard to a geographical area which included the Domicilio apartment complex. This area may have been larger or smaller than the entirety of the Domicilio property. Once this area was identified, FBI technical agents stopped using the StingRay and then used the KingFish to pinpoint the precise location of the aircard.

996. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 063 of *2nd Consolidated Exhibits* (Dkt. #821-3) (July 17, 2008, 12:53am, text message sent from FBI Agent Murray to FBI Agent Killigrew).

997. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., EXHIBIT 064 of *2nd Consolidated Exhibits* (Dkt. #821-3) (July 17, 2008, 2:42am, text message sent from FBI technical agent to unknown individual).

factually assume, that, at the conclusion of the July 16, 2008, aircard tracking operation, the FBI located the aircard within Unit 1122 of the Domocilio [sic] Apartments."[998]

i. Whenever the aircard was connected to either the StingRay or KingFish, the FBI denied the aircard access to the Internet (*i.e.*, a denial-of-service attack).

62. Immediately after the aircard established a session with the FBI's StingRay or KingFish, the user, believing he was connected to a Verizon Wireless cell site, attempted to connect his aircard and laptop computer to the aircard Internet access service.[999] Because the StingRay and KingFish are not capable of forwarding communications content to Verizon Wireless,[1000] the aircard user was not provided with any type of Internet access service.[1001] From approximately 5:03pm on July 16, 2008 (time at which the last surreptitious phone call was placed to the aircard)[1002] to approximately 2:42am on July 17, 2008 (time at which the

998. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Government's Memorandum RE Motion For Discovery* (Dkt. #674, p. 2) (footnote omitted).

999. United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection* (Dkt. #824-3, ¶ 17-20, p. 6-7) (explaining my standard practice to immediately initiate a connection with Verizon Wireless whenever I plug my aircard into my laptop computer).

1000. *See How The Aircard Was Intruded Upon*, Section IV(A)(2)(a), *supra* (explaining how the Harris StingRay and KingFish are incapable of conducting man-in-the-middle-attacks).

1001. The government conceded that the equipment used by the FBI technical agents "caused a brief disruption in service to the aircard." United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court Order* (Dkt. #723, p. 14). I do not agree with the government's limited concession. The evidence shows that the FBI technical agents caused an **extensive** disruption in service, *i.e.*, first for a six (6) hour period using surreptitious phone calls (*see How The Aircard Was Intruded Upon*, Section IV(B)(8), *supra*) followed by a ten (10) hour period using the StingRay and KingFish (*see How The Aircard Was Intruded Upon*, Section IV(B)(9)(i), *supra*).

1002. *See How The Aircard Was Intruded Upon*, Section IV(B)(9)(a), *supra*.

KingFish pinpointed the aircard inside apartment No. 1122),[1003] the aircard user was denied access to the Internet by the FBI. Using the StingRay and KingFish, the FBI technical agents conducted a denial-of-service attack on the aircard for almost a 10 hour period.

j. The FBI's StingRay and KingFish relied upon the electricity provided to the aircard by its user.

63. In order for radio waves to be transmitted from a wireless device, they require a power source of which to draw electricity. Once transmitted, the radio waves carry the energy drawn from the power source to the receive antenna of the destination radio receiver.[1004] The receive antenna uses the transmitted energy to decode the radio waves into readable signals.[1005] Without the energy that originated at the transmit antenna, the receiver would be unable to receive, let alone decode, the transmitted signals.

64. Because the FBI technical agents were forcing the aircard to generate and transmit radio waves that were subsequently collected and decoded by their surveillance equipment, the FBI was relying upon the electricity being provided to the aircard. The aircard received its power from the host laptop computer,[1006] which in turn received its power from a wall outlet within apartment No. 1122.[1007] The electricity flowing from the wall outlet was

1003. *See id.*, Section IV(B)(9)(h), *supra*.

1004. *See Technical Explanations*, Section III(A), *supra*, and fn. Nos. 29-30.

1005. *See id*.

1006. *See How The Aircard Was Intruded Upon*, Section IV(A)(1), *supra* (general background information on the aircard and host laptop computer).

1007. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., defendant's declaration RE: *Daniel Rigmaiden's residence was at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA. 95050* (Dkt. #824-2, ¶ 11-12, p. 3-4).

purchased by the aircard user from Silicon Valley Power via a utility account.[1008] The FBI technical agents were hijacking the aircard user's electricity for use in their aircard locating mission.

k. The FBI's StingRay and KingFish sent the aircard commands instructing it to increase its signal transmission power to facilitate more effective geolocation.

65. The FBI technical agents were also forcing the aircard to transmit at the highest possible power[1009] thus increasing the amount of electricity hijacked from apartment No. 1122. One feature of the StingRay and KingFish while emulating 1xEV-DO Rel. 0 cell sites is the ability to transmit closed-loop Reverse Power Control (RPC) bits to a target wireless device.[1010] By transmitting enough RPC bits, the FBI's equipment can force a wireless device to transmit at the highest possible power so that the collected location finding response signals are easier to measure.[1011] In order to more precisely search for and locate the aircard while using its StingRay and KingFish, the FBI technical agents sent RPC bits to the aircard causing it to transmit at a higher power than it would have normally transmitted if it were accessing cellular service through an actual Verizon Wireless cell site covering apartment No. 1122.

1008. *See id.*, ¶ 11, p. 3.

1009. *See Technical Explanations*, Section III(G)(1)(b)(vi), *supra* (explaining forced transmission power increase as used by the StingRay and KingFish to locate wireless devices).

1010. *See id.*, Section III(B)(3)(e)(ii), *supra* (explaining 1xEV-DO Rel. 0 closed-loop power control on the Reverse Traffic Channel).

1011. *See id.*, Section III(G)(1)(b)(vi), *supra* (explaining forced transmission power increase as used by the StingRay and KingFish to locate wireless devices).

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

V. Daniel Rigmaiden's Expert Qualifications

I am as qualified an expert as the sources cited in this declaration. I have read every cited Telecommunications Industry Association Engineering Standard/Publication—front to back—as well as large sections of all cited technical books and a number of other technical resources not cited. I spent approximately seven hundred (700) hours over approximately seven (7) months (*i.e.*, November of 2011 through May of 2012) reviewing more than 10,000 pages of Telecommunications Industry Association documents and other resources in order to draft the content of this declaration.

After my original submission of the information contained in this declaration,[1012] Kim Zetter of Wired Magazine wrote an article explaining cell site emulator technology based on my technical conclusions.[1013] In Kim Zetter's article, my technical conclusions were cited and quoted numerous times.[1014]

In United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., the Court noted that I have an "extensive command of technical information[.]"[1015] The Court also found that the government withheld discoverable evidence relating to the cell site emulators used to intrude

1012. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *Motion To Suppress, Memorandum RE: Fourth Amendment Violations* (Dkt. #824-1).

1013. *See* Zetter, Kim, wired.com [website], *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight | Threat Level | Wired.com* (Apr. 9, 2013), http://www.wired.com/threatlevel/2013/04/verizon-rigmaiden-aircard/all/ (last accessed: Apr. 10, 2013).

1014. *See id*.

1015. *See* United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *January 4, 2012 Court*

upon and locate the aircard.[1016] Because evidence was withheld, the Court indicated that the government would not be permitted to present its own expert or agent, or use other means not involving the disclosure of evidence, to rebut my self-collected evidence and technical explanations regarding the operations of cell site emulators:

> [THE COURT:] ... Now, if I were to conclude that the method by which the device works is privileged, and if I were also to conclude that the government doesn't have to produce[, for example,] the details of whether it writes software to the laptop or boosts the signal of the aircard because Mr. Rigmaiden has other means for making that argument, then it seems to me when we get to the suppression hearing, this is what's likely to happen:
>
> Mr. Rigmaiden will present evidence, as he has in his motion, that the device the government uses boosts the signal strength and writes software to the hard drive, and he has evidence from the Harris products criteria. He's got evidence from government documents. He's pulled it from a number of different sources.
>
> The government at that suppression hearing could not respond by saying, "No, here's how it works," because you've withheld that information. Therefore, I would find by a preponderance of the evidence that he's right, that this device does, in fact, boost the signal and does write software to the laptop. And I would take that factual finding into account when I ruled on the motion to suppress because I would find by a preponderance of the evidence, which is all that is needed, he's shown that that's what this kind of a device does.
>
> If the government were at the suppression hearing to say, "Well, we're not going to put any of the sensitive information into evidence but we want to call an expert or an agent to testify that most of these devices don't do that, they don't boost signal strength, they don't write software to the laptop," it seems to me that I need to do one of two things. I either need to say, "Well, if you're saying most of them don't but some of them do, then you've got to give him the evidence with which he can figure out whether this one does," or I've got to find in his favor on this question of fact because he's presented evidence that that's how the device

Order (Dkt. #723, p. 29-30).

1016. *See id.* (Dkt. #723) (denying defendant access to discoverable evidence based on government's claim of law "enforcement privilege").

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

> works. You haven't ruled it out with your evidence because some do that. So by a preponderance of the evidence I will find that the device in this case boosts signal strength and writes software to the laptop.
>
> Now, if we were to go to that point, it seems to me that Mr. Rigmaiden's rights would not have been compromised because he's been able to make the point as to how the device works, and I'm accepting it as true by a preponderance of the evidence. The government couldn't complain because it withheld the information with which it could disprove that if, in fact, it could disprove it.
>
> United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., *September 22, 2011 Motion Hearing, Partial Transcript of Proceedings*, p. 10-11.

Therefore, at the very least, I am qualified as a cdma2000 1xEV-DO Rel. 0 expert, cell site emulator expert, and geolocation expert in the context of the government intruding upon the aircard in United States v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz.[1017]

* * * * *

I declare, certify, verify, and state under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge, except as to those matters which are therein stated on information and belief, and, as to those matters, I believe it to be true. *See* 28 U.S.C. § 1746 ("Wherever... any matter is required or permitted to be supported, evidenced, established, or proved by the sworn... affidavit, in writing of the person making the same [], such matter may, with like force and effect, be supported, evidenced, established, or proved by the unsworn declaration..., in writing of such person which is subscribed by him, as true under penalty of perjury, and dated..."); 18 U.S.C. § 1621 ("Whoever... in any declaration... under penalty of perjury as permitted under section 1746 of

1017. *See* Masterson Marketting, Inc. v. KSL Recreation Corp., 495 F. Supp. 2d 1044, 1050 (S.D.Cal. 2007) (Noting that "a party who is otherwise qualified as an expert may testify as an expert witness in his own case regardless of concerns that the party is plainly self-interested.").

DECLARATION UNDER PENALTY OF PERJURY

RE: The independent operations of the FBI's cell site emulators, etc. used to locate the UTStarcom PC5740 1xEV-DO aircard in United States v. Rigmaiden, CR08-814-PHX-DGC (D.Ariz.);

BY: Daniel David Rigmaiden

---

title 28, United States Code, willfully subscribes as true any material matter which he does not believe to be true... is guilty of perjury and shall, except as otherwise expressly provided by law, be fined under this title or imprisoned not more than five years, or both....").

Executed on May 29, 2013, in Florence, Arizona, United States of America.

Daniel David Rigmaiden

Daniel Rigmaiden

Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132